РОСЭНЕРГОАТОМ
ЭЛЕКТРОЭНЕРГЕТИЧЕСКИЙ ДИВИЗИОН РОСАТОМА

Акционерное общество
«Российский концерн по производству электрической
и тепловой энергии на атомных станциях»

(АО «Концерн Росэнергоатом»)

ПРИКАЗ

28.06.2018 № 9/791-П

Москва

О введении в действие ОТТ 1.1.3.10.1446-2018

В целях реализации Плана мероприятий по подготовке к корпоративной миссии ОСАРТ по направлению «Корпоративная техническая поддержка» (указание АО «Концерн Росэнергоатом» от 24.05.2017 № 9/95-У) пересмотрены ОТТ 1.1.8.07.1169-2016 «Атомные станции. Управляющие системы, важные для безопасности. Создание, модернизация и эксплуатация. Общие технические требования» (приказ АО «Концерн Росэнергоатом» от 16.03.2017 № 9/342-П).

На основании изложенного

ПРИКАЗЫВАЮ:

1. Ввести в действие с 20.08.2018 ОТТ 1.1.3.10.1446-2018 «Атомные станции. Управляющие системы, важные для безопасности. Создание, модернизация и эксплуатация. Общие технические требования» (далее – ОТТ 1.1.3.10.1446-2018, приложение).

2. Заместителям Генерального директора – директорам филиалов АО «Концерн Росэнергоатом» (далее – Концерн) – действующих атомных станций, директорам филиалов Концерна – дирекций строящихся атомных станций, заместителю директора по производству и эксплуатации АЭС – директору Департамента по эксплуатационной готовности новых АЭС Кацману А.М. принять ОТТ 1.1.3.10.1446-2018 к руководству и исполнению.

3. Департаменту планирования производства, модернизации и продления срока эксплуатации (Максимов Ю.М.) внести в установленном порядке ОТТ 1.1.3.10.1446-2018 в подраздел 1.14.1 части III Указателя технических документов, регламентирующих обеспечение безопасности на всех этапах жизненного цикла атомных станций (обязательных и рекомендуемых к использованию).

gost.e-ecolog.ru

УД/32871/26.06

4. Департаменту по эксплуатационной готовности новых АЭС (Кацман А.М.) обеспечить координацию работ по внедрению ОТТ 1.1.3.10.1446-2018.

5. Признать утратившим силу с 20.08.2018 приказ Концерна от 16.03.2017 № 9/342-П «О введении в действие ОТТ 1.1.8.07.1169-2016».

И. о. Генерального директора А.В. Шутиков

С.В. Маяков
+7 (495) 783-01-43 / 15-32

Приложение к приказу
АО «Концерн Росэнергоатом»
от 22.06.2018 № 9/791-П

РОСЭНЕРГОАТОМ
ЭЛЕКТРОЭНЕРГЕТИЧЕСКИЙ ДИВИЗИОН РОСАТОМА

Акционерное общество
«Российский концерн по производству электрической и тепловой энергии на атомных станциях»

(АО «Концерн Росэнергоатом»)

УТВЕРЖДАЮ

И. о. заместителя Генерального директора – директора по производству и эксплуатации АЭС

_____ А.Г. Крупский

«13» 06 2018

АТОМНЫЕ СТАНЦИИ

УПРАВЛЯЮЩИЕ СИСТЕМЫ, ВАЖНЫЕ ДЛЯ БЕЗОПАСНОСТИ. СОЗДАНИЕ, МОДЕРНИЗАЦИЯ И ЭКСПЛУАТАЦИЯ

Общие технические требования

ОТТ 1.1.3.10.1446-2018

Предисловие

1 РАЗРАБОТАНЫ Департаментом по эксплуатационной готовности новых АЭС

2 ВНЕСЕНЫ Департаментом по эксплуатационной готовности новых АЭС

3 ВВЕДЕНЫ В ДЕЙСТВИЕ приказом АО «Концерн Росэнергоатом» от 28.06. 2018 № 9/791-П

4 ВЗАМЕН ОТТ 1.1.8.07.1169-2016

Содержание

1 Область применения 1

2 Нормативные ссылки 2

3 Термины и определения 5

4 Сокращения 16

5 Проектирование управляющих систем, важных для безопасности 19

5.1 Основные требования к управляющим системам важным для безопасности...19

5.2 Разработка архитектуры СКУ энергоблока АС 23

6 Разработка управляющих систем, важных для безопасности 27

6.1 Этапы разработки 28

6.2 Техническое задание на систему 29

6.3 Требования к функциям системы 32

6.4 Разработка технических средств системы 41

6.5 Разработка программных средств системы 43

6.6 Модификации 57

7 Квалификация оборудования 57

7.1 Общие положения 57

7.2 Порядок проведения квалификации 59

7.3 Квалификация оборудования прямым испытанием 60

7.4 Квалификация оборудования опытом эксплуатации 66

7.5 Квалификация оборудования на основе анализа 68

7.6 Комбинированная квалификация 69

7.7 Квалификация работающего оборудования 70

7.8 Критерии отказа 71

7.9 Отчет о проведении квалификации оборудования 71

7.10 Определение категории квалификации оборудования 72

8 Разработка пунктов управления 76

8.1 Общие требования к пунктам управления 76

8.2 Общие требования к человеко-машинному интерфейсу 82

8.3 Средства управления 85

8.4 Средства отображения информации на РС 86

8.5 Контроль аварийных условий 90

8.6 Система сигнализации 92

8.7 Системы регистрации хронологических данных 93

9 Полигонные испытания. Общие технические требования 94

9.1 Общие сведения 94

9.2 Условия проведения комплексных полигонных испытаний 95

9.3 Цели и критерии оценки комплексных полигонных испытаний 97

9.4 Требования к содержанию программ и методик комплексных испытаний 102

9.5 Организация и проведение комплексных полигонных испытаний 105

10 Монтаж средств автоматизации управляющих систем 107

10.1 Общие требования 107

10.2 Подготовка к производству монтажных работ 108

10.3 Приемка объекта под монтаж 112

10.4 Передача в монтаж средств автоматизации, изделий, материалов и технической документации 116

10.5 Производство монтажных работ 117

10.6 Индивидуальные испытания и приемка средств автоматизации из монтажа .119

11 Ввод управляющих систем в эксплуатацию 121

12 Эксплуатация управляющих систем энергоблока АС 121

12.1 Организация эксплуатации 121
13 Внесение изменений в УСВБ 133
13.1 Общие положения 133
13.2 Основание и цели внесения изменений 134
13.3 Классификация изменений 134
13.4 Порядок внесения изменений, не требующих корректировки проектной документации 138
13.5 Порядок внесения изменений, требующих корректировки проектной, рабочей или конструкторской документации 139
14 Модернизация 142
15 Обеспечение информационной безопасности 142
15.1 Общие требования к информационной безопасности СКУ АС 142
15.2 Основные требования на этапе проектирования 143
15.3 Основные требования на этапе конструирования 143
15.4 Основные требования на этапе изготовления 144
15.5 Приемо-сдаточные испытания СКУ в части ИБ 145
Библиография 146

АТОМНЫЕ СТАНЦИИ. УПРАВЛЯЮЩИЕ СИСТЕМЫ, ВАЖНЫЕ ДЛЯ БЕЗОПАСНОСТИ. СОЗДАНИЕ, МОДЕРНИЗАЦИЯ И ЭКСПЛУАТАЦИЯ. Общие технические требования

Дата введения с 20.08.2018

1 Область применения

1.1 Настоящие общие технические требования устанавливают основные требования к управляющим системам (элементам систем), важным для безопасности атомных станций (УСВБ АС), а также процессам их создания, модернизации и эксплуатации.

1.2 Настоящие общие технические требования разработаны с учетом требований НП-001, НП-026, а также других нормативных документов, действующих в атомной энергетике.

1.3 Настоящие общие технические требования предназначены для применения эксплуатирующей организацией АО «Концерн Росэнергоатом» (далее – Концерн), научно-исследовательскими, проектными, конструкторскими, наладочными предприятиями, изготовителями управляющих систем (элементов систем) важных для безопасности атомных станций.

1.4 Настоящие общие технические требования распространяются на:

– управляющие системы (элементы систем), важные для безопасности, проектируемых энергоблоков АС;

– управляющие системы (элементы систем), важные для безопасности вновь создаваемые или модернизируемые на действующих энергоблоках в соответствии с решениями, оформленными в установленном порядке;

– управляющие системы (элементы систем), важные для безопасности, действующих энергоблоков в объеме требований разделов «Эксплуатация управляющих систем энергоблока АЭС», «Внесение изменений в УСВБ».

2 Нормативные ссылки

В настоящих общих технических требованиях использованы ссылки на следующие нормативные документы:

НП-001-15 Общие положения обеспечения безопасности атомных станций

НП-026-16 Требования к управляющим системам, важным для безопасности атомных станций

НП-071-18 Правила оценки соответствия продукции, для которой устанавливаются требования, связанные с обеспечением безопасности в области использования атомной энергии, а также процессов ее проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации, утилизации и захоронения

НП-082-07 Правила ядерной безопасности реакторных установок атомных станций

НПБ 160-97 Цвета сигнальные. Знаки пожарной безопасности. Виды, размеры, общие технические требования

СНиП 3.05.07-85 Свод правил. Системы автоматизации

СанПин 2.6.1.24-03 Санитарные правила проектирования и эксплуатации атомных станций (СП АС-03)

ГОСТ 2.105-95 Единая система конструкторской документации (ЕСКД). Общие требования к текстовым документам

ГОСТ 2.114-2016 Единая система конструкторской документации (ЕСКД). Технические условия

ГОСТ 2.601-2013 Единая система конструкторской документации (ЕСКД). Эксплуатационные документы

ГОСТ 2.503-2013 Единая система конструкторской документации (ЕСКД). Правила внесения изменений

ГОСТ 15.309-98 Система разработки и постановки продукции на производство (СРПП). Испытания и приемка выпускаемой продукции. Основные положения

ГОСТ 19.603-78 Единая система программной документации (ЕСПД). Общие правила внесения изменений

ГОСТ 34.003-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения

ГОСТ 34.602-89 Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы

ГОСТ 34.603-92 Информационная технология. Виды испытаний автоматизированных систем

ГОСТ 28195-89 Оценка качества программных средств. Общие положения

ГОСТ 32137-2013 Совместимость технических средств электромагнитная. Технические средства для атомных станций. Требования и методы испытаний

ГОСТ Р 15.301-2016 Система разработки и постановки продукции на производство (СРПП). Продукция производственно-технического назначения. Порядок разработки и постановки продукции на производство

ГОСТ Р 51317.4.1-2000 Совместимость технических средств электромагнитная. Испытания на помехоустойчивость. Виды испытаний

ГОСТ Р МЭК 60880-2010 Атомные электростанции. Системы контроля и управления, важные для безопасности. Программное обеспечение компьютерных систем, выполняющих функции категории А

ГОСТ Р МЭК 60964-2012 Атомные станции. Пункты управления. Проектирование

ГОСТ Р МЭК 61225-2011 Атомные станции. Системы контроля и управления, важные для безопасности. Требования к электроснабжению

ГОСТ Р МЭК 61298-2-2015 Приборы измерения и управления промышленным процессом. Общие методы и процедуры оценки рабочих характеристик. Часть 2. Испытания при нормальных условиях

ГОСТ Р МЭК 61508-4-2012 Функциональная безопасность систем электрических, электронных, программируемых электронных связанных с безопасностью. Часть 4. Термины и определения

ГОСТ Р МЭК 61513-2011 Атомные станции. Системы контроля и управления, важные для безопасности. Общие положения

Правила устройства электроустановок (ПУЭ)

Правила по охране труда при эксплуатации электроустановок

Правила по охране труда при работе с инструментом и приспособлениями

СТО 1.1.1.01.0678-2015 Основные правила обеспечения эксплуатации атомных станций

СТО 1.1.1.03.003.0914-2013 Ввод в эксплуатацию блоков атомных станций с водо-водяными энергетическими реакторами. Порядок выполнения и приемки посконаладочных работ на АСУ ТП

СТО 1.1.1.03.003.0916-2013 Правила ввода блоков атомных станций в эксплуатацию

СТО 1.1.1.04.003.0542-2014 Порядок организации и проведения модернизации систем и оборудования

РД ЭО 1.1.2.01.0713-2013 Положение об оценке соответствия в форме приемки и испытаний продукции для атомных станций

РД ЭО 1.1.2.01.0958-2014 Согласование технических требований и решений о применении импортной продукции, предназначенной для использования на атомных станциях. Положение

РД ЭО 1.1.2.01.0740-2012 Техническая документация. Положение о порядке разработки, регистрации и учета решений (технических решений)

РБ-004-98 Требования к сертификации управляющих систем, важных для безопасности атомных станций

ОТТ 08042462 Приборы и средства автоматизации для атомных станций. Общие технические требования

РД 50-34.698-90 Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Требования к содержанию документов

Примечание - При пользовании настоящими общими техническими требованиями необходимо проверить актуальность нормативных документов, указанных в настоящем разделе (далее – Нормативные документы). Если Нормативные документы заменены (изменены), то при пользовании настоящими общими техническими требованиями необходимо применять заменяющие (измененные) нормативные документы. Если Нормативные документы отменены без замены, то положения настоящих общих технических требований, в которых даны ссылки на эти документы, применяются в части, не затрагивающей эти ссылки.

3 Термины и определения

В настоящих общих технических требованиях применены следующие термины с соответствующими определениями:

3.1 **авария на АС (авария)**: Нарушение нормальной эксплуатации АС, при котором произошел выход радиоактивных веществ и (или) ионизирующего излучения за границы, предусмотренные проектной документацией АС для нормальной эксплуатации в количествах, превышающих установленные пределы безопасной эксплуатации; авария характеризуется исходным событием, путями протекания и последствиями (НП-001).

3.2 **архитектура контроля и управления**: Организованная структура систем контроля и управления АС, которые являются важными для безопасности (ГОСТ Р МЭК 61513).

3.3 **архитектура системы контроля и управления**: Организованная структура системы контроля и управления (ГОСТ Р МЭК 61513).

3.4 **безопасность АС (ядерная и радиационная безопасность АС)**: Свойство АС обеспечивать надежную защиту персонала, населения и окружающей среды от недопустимого в соответствии с федеральными нормами и правилами в области использования атомной энергии радиационного воздействия (НП-001).

3.5 **блочный пункт управления**: Часть блока АС, размещаемая в специально предусмотренных проектом АС помещениях и предназначенная для централизованного автоматизированного управления технологическими

процессами, реализуемого оперативным персоналом и средствами автоматизации (НП-001).

3.6 **валидация системы**: Подтверждение путем проверки и предоставления других свидетельств того, что система в целом соответствует спецификации требований (функциональность, время отклика, устойчивость к дефектам и ошибкам, запас прочности) (ГОСТ Р МЭК 60880).

3.7 **верификация**: Подтверждение путем проверки и предоставления объективных свидетельств того, что результаты деятельности соответствуют целям и требованиям, определенным для этой деятельности (ГОСТ Р МЭК 60880).

3.8 **ввод в эксплуатацию блока АС**: Процесс, во время которого системы и оборудование АС (блока АС) начинают функционировать, а также проверяются их соответствие проекту АС и готовность к эксплуатации, завершающийся получением в установленном градостроительным законодательством порядке разрешения на ввод объекта в эксплуатацию. Ввод в эксплуатацию блока АС разделяется на этапы: предпусковые наладочные работы, физический пуск, энергетический пуск, опытно-промышленная эксплуатация (НП-001).

3.9 **дефект программного обеспечения**: Ошибка программирования, содержащаяся в одном из компонентов программного обеспечения (ГОСТ Р МЭК 61513).

3.10 **диагностика**: Функция контроля, целью которой является определение состояния работоспособности (неработоспособности) или исправности (неисправности) диагностируемого объекта (НП-082).

3.11 **единичный отказ**: Случайный отказ, который выражается в потере способности элемента системы или системы выполнять предписанные функции. Отказы, возникающие как следствие единичного случайного события, рассматриваются как составляющие единичного отказа (ГОСТ Р МЭК 61513).

3.12 **жизненный цикл ПО**: Процессы, происходящие в течение периода времени, который начинается с появления общей концепции программного обеспечения и заканчивается если программное обеспечение окончательно выведено из эксплуатации (ГОСТ Р МЭК 61508-4).

3.13 **жизненный цикл систем безопасности:** Необходимые процессы, относящиеся к реализации систем, связанных с безопасностью, проходящие в течение периода времени, начиная со стадии разработки концепции проекта и заканчивая стадией, когда все системы, связанные с безопасностью, и другие средства снижения риска уже не используются (ГОСТ Р МЭК 61508-4).

3.14 **зависимый отказ:** Отказ системы (элемента), являющийся следствием другого отказа или события (НП-001).

3.15 **запроектная авария**: Авария, вызванная не учитываемыми для проектных аварий исходными событиями или сопровождающаяся дополнительными по сравнению с проектными авариями отказами элементов систем безопасности сверх единичного отказа, реализацией ошибочных решений персонала (НП-001).

3.16 **исходное событие:** Единичный отказ в системе (элементе) АС, внутреннее или внешнее воздействие, или ошибка персонала, либо сочетания указанных событий, которые приводят к нарушению нормальной эксплуатации АС и могут привести к нарушению пределов и (или) условий безопасной эксплуатации (НП-001-15).

3.17 **канал:** Ряд взаимосвязанных компонентов внутри системы, которые формируют один выходной сигнал. Канал теряет свою индивидуальность, если его выходные сигналы сочетаются с сигналами от другого канала, например, канала контроля или канала безопасности (ГОСТ Р МЭК 61513).

3.18 **канал системы:** Часть системы, выполняющая в заданном проектом АС объеме функцию системы (НП-001).

3.19 **квалификация персонала (квалификация)**: Уровень подготовленности лица из числа руководителей и работников АС и других организаций, выполняющих работы, оказывающие влияние на безопасность АС, включая базовое специальное образование, профессиональные знания, навыки и умения, а также опыт работы, обеспечивающий качество и безопасность эксплуатации АС при выполнении должностных обязанностей (НП-001).

3.20 **квалификация оборудования:** Подтверждение посредством анализа, типовых испытаний или опыта эксплуатации того, что при требуемых

эксплуатационных и внешних условиях оборудование способно выполнить свои функции с необходимой точностью и с сохранением требуемых характеристик IEC/IEEE 60780-323 [1]).

3.21 **комплекс безопасности:** Взаимосвязанный набор оборудования, спроектированный для выполнения всех операций, необходимых для того, чтобы гарантировать непревышение пределов, установленных проектом для данного исходного события (ГОСТ Р МЭК 61513).

3.22 **комплекс технических средств**: Комплекс, представляющий совокупность технических средств автоматизации, предназначенных для реализации управляющих технических систем (РБ-004).

3.23 **контроль:** Часть функции управления, целью которой является оценка значения (идентификация) параметра или определение состояния контролируемого процесса или оборудования.

3.24 **критерий единичного отказа:** Критерий (или требование), применяемый к системе таким образом, чтобы она обязательно сохраняла способность выполнять свою функцию в случае любого единичного отказа.

3.25 **квалификационный запас:** Разница между наиболее жесткими эксплуатационными условиями, заданными для оборудования, и условиями, применяемыми при его квалификационных испытаниях.

3.26 **манипулятор:** Техническое средство/устройство, предназначенное для передачи управляющих воздействий от оператора к управляющей системе.

3.27 **мнемосхема:** Средство отображения информации, с помощью которого в наглядном виде воспроизводится структура и динамика состояний объекта или процесса.

3.28 **модернизация:** Работы по изменению технологических или служебных характеристик оборудования, зданий, сооружений или иных объектов амортизируемых основных средств, направленные на достижения более высоких показателей при эксплуатации, включая улучшение проектных, либо реально достигнутых показателей функционирования (срок полезного использования, мощность, надежность, качество применения и т.п.).

3.29 **модификация программного средства:** Вносимые в согласованную программную документацию изменения, которые приводят к изменению исполнительных кодов или данных.

3.30 **надежность:** Вероятность того, что прибор, система или устройство будут выполнять назначенные функции удовлетворительно в течение определенного времени в определенных условиях эксплуатации (ГОСТ Р МЭК 61513).

3.31 **надежность программного обеспечения:** Составляющая надежности системы, которая зависит от отказов программного обеспечения (ГОСТ Р МЭК 61513).

3.32 **нарушение нормальной эксплуатации:** Нарушение в работе АС, при котором произошло отклонение от установленных эксплуатационных пределов и (или) условий. При этом могут быть нарушены и другие установленные проектом АС пределы и (или) условия, включая пределы и (или) условия безопасной эксплуатации (НП-001).

3.33 **нормальная эксплуатация:** Эксплуатация АС в определенных проектом эксплуатационных пределах и условиях (НП-001).

3.34 **обеспечивающие системы (элементы) безопасности:** Системы (элементы), предназначенные для снабжения систем безопасности энергией, рабочей средой и создания условий для их функционирования (НП-001).

3.35 **образец оборудования:** Промышленный комплект оборудования, на котором проводят испытания и получают данные, пригодные для оценки целого ряда его параметров (IEC/IEEE 60780-323 [1]).

3.36 **опытно-промышленная эксплуатация:** Этап ввода АС (блока АС) в эксплуатацию после энергетического пуска, завершающийся получением в установленном порядке разрешения эксплуатировать блок АС (НП-001).

3.37 **основная характеристика:** Любой внутренний физический параметр, относящийся к свойствам материалов или к проекту оборудования, который влияет на эксплуатационные характеристики оборудования, когда достигаются максимальные допустимые значения или общепринятые максимальные значения. Сюда относится диапазон температуры для материалов, магнитные поля и т.д.

3.38 **отказ оборудования:** Событие, заключающееся в нарушении работоспособного состояния оборудования.

3.39 **отказ по общей причине:** Отказ двух или более структур, систем или компонентов вследствие одного конкретного события или одной конкретной причины (ГОСТ Р МЭК 60880).

3.40 **ошибка персонала:** Единичное непреднамеренное неправильное действие или единичный пропуск правильного действия при управлении системами и элементами АС, или единичное непреднамеренное неправильное действие, или пропуск правильного действия при техническом обслуживании или ремонте систем и элементов АС (НП-001).

3.41 **отказ программного обеспечения:** Отказ системы из-за проявившейся проектной ошибки в компоненте программного обеспечения.

3.42 **предаварийная ситуация:** Нарушение пределов и (или) условий безопасной эксплуатации, не перешедшее в аварию (НП-001).

3.43 **пределы безопасной эксплуатации АС:** Установленные проектом АС значения параметров технологического процесса, отклонения от которых могут привести к аварии.

Различают пределы безопасной эксплуатации по радиационным параметрам и пределы безопасной эксплуатации по другим технологическим параметрам. Нарушение пределов безопасной эксплуатации по радиационным параметрам является аварией (НП-001).

3.44 **предпусковые наладочные работы**: Этап ввода блока АС в эксплуатацию, в ходе которого законченные строительством и монтажом системы и элементы АС приводятся в состояние эксплуатационной готовности с проверкой их соответствия установленным в проекте АС критериям и характеристикам, завершающийся готовностью блока АС к этапу физического пуска (НП-001).

3.45 **прикладная функция:** Функция системы контроля и управления, выполняющая задачу, связанную с контролируемым процессом, а не с функционированием самой системы (ГОСТ Р МЭК 60880).

3.46 **прикладное программное обеспечение:** Часть программного обеспечения системы контроля и управления, которая обеспечивает выполнение прикладных функций (ГОСТ Р МЭК 60880).

3.47 **принцип независимости**: Принцип повышения надежности путем применения функционального и (или) физического разделения каналов (элементов), при котором отказ одного канала (элемента) не приводит к отказу другого канала (элемента) (НП-001).

3.48 **принцип разнообразия**: Принцип повышения надежности путем применения двух или более систем или элементов для выполнения одной функции безопасности, имеющих различные конструкции или принципы действия, имеющий целью снижение вероятности отказа по общей причине (НП-001).

3.49 **принцип резервирования (избыточности)**: Принцип повышения надежности путем применения нескольких одинаковых или неодинаковых элементов (каналов, систем) таким образом, чтобы каждый из них мог выполнить требуемую функцию независимо от состояния, в том числе отказа, других элементов (каналов, систем), предназначенных для выполнения этой функции (НП-001).

3.50 **проектная авария**: Авария, для которой в проекте АС определены исходные события и конечные состояния и предусмотрены системы безопасности, обеспечивающие при независимом от исходного события отказе одного из элементов систем безопасности, учитываемом в проекте АС, или при одной, независимой от исходного события, ошибке персонала ограничение ее последствий установленными для таких аварий пределами (НП-001).

3.51 **разнообразие:** Существование двух или более путей или средств достижения установленной цели. Разнообразие специально создается как защита от отказа по общей причине. Оно может быть достигнуто за счет использования систем, которые физически отличаются одна от другой, или с помощью функционального разнообразия, когда аналогичные системы достигают установленной цели различными путями (ГОСТ Р МЭК 60880).

3.52 **разработчики проекта АС (РУ):** Организации, разрабатывающие проект АС (РУ) и обеспечивающие его научно-техническое, в том числе

конструкторское, сопровождение на всех этапах полного жизненного цикла АС (РУ) (НП-001).

3.53 **ранее разработанное программное обеспечение:** Часть программного обеспечения, которое уже существует, доступна в качестве коммерческой или патентованной программы и предполагается к использованию (ГОСТ Р МЭК 60880).

3.54 **регистрация:** Информационная функция, целью которой является фиксация информации на каком-либо носителе, позволяющем ее хранение.

3.55 **резервирование:** Наличие альтернативных (идентичных или различных) элементов или систем с тем, чтобы любой из них мог выполнять необходимую функцию независимо от рабочего состояния или отказа любого другого (ГОСТ Р МЭК 60880).

3.56 **ремонтопригодность:** Вероятность того, что определенная операция по обслуживанию устройства в данных условиях эксплуатации может быть выполнена в заранее определенный период времени, в заранее определенных условиях с использованием заранее определенных операций и средств.

3.57 **система АС (система)**: Совокупность элементов АС, предназначенная для выполнения заданных функций (НП-001).

3.58 **система контроля и управления:** Система, основанная на применении электрической и/или электронной и/или программируемой электронной техники, выполняющая функции контроля и управления, а также функции обслуживания и наблюдения, связанные с эксплуатацией самой системы. Термин используется как обобщающий, охватывающий все элементы системы, включая питание, датчики и другие входные устройства, лини передачи данных и другие связи, интерфейсы исполнительных устройств и других выходных устройств. Различные функции системы могут использовать как выделенные, так и разделенные ресурсы (ГОСТ Р МЭК 61513).

3.59 **систематический отказ**: Отказ, связанный детерминированным образом с какой-либо причиной, которая может быть исключена только путем модификации проекта либо производственного процесса, операций, документации, либо других факторов (ГОСТ Р МЭК 61508-4).

3.60 **системное программное обеспечение:** Программное обеспечение, спроектированное для определенной компьютерной системы или семейства компьютерных систем с целью эксплуатации и обслуживания компьютерной системы и установленных программ, например, операционные системы, ЭВМ, утилиты. Системное программное обеспечение обычно состоит из операционного системного программного обеспечения и инструментальных программ (ГОСТ Р МЭК 61513).

3.61 **системы (элементы) безопасности**: Системы (элементы), предназначенные для выполнения функций безопасности при проектных авариях (НП-001).

3.62 **система управления и защиты:** Совокупность средств технического, программного и информационного обеспечения, предназначенная для обеспечения безопасного протекания цепной ядерной реакции деления (система, важная для безопасности, совмещающая функции нормальной эксплуатации и безопасности и состоящая из элементов управляющих систем нормальной эксплуатации, защитных, управляющих и обеспечивающих систем безопасности) (НП-082).

3.63 **средства автоматизации:** Совокупность программных, технических и программно-технических средств, предназначенных для создания управляющих систем (РБ-004).

3.64 **средство отображения:** Устройство в системе «человек-машина», предназначенное для восприятия оператором сигналов о состоянии объекта воздействия, системы «человек-машина» и способов управления ими (ГОСТ 34.003).

3.65 **старение (естественное):** Изменение со временем физических, химических или электрических свойств оборудования или его компонентов при работе в проектных условиях эксплуатации, которые могут привести к ухудшению основных технических характеристик оборудования (IEC/IEEE 60780-323 [1]).

3.66 **типовые испытания:** Испытания, проводимые на образцах оборудования с целью подтверждения соответствия оборудования предъявляемым к нему требованиям.

3.67 **техническое обслуживание**: Комплекс операций по поддержанию работоспособности и исправности объекта (систем и элементов) при использовании по назначению, в режиме ожидания, при хранении и транспортировании (НП-001).

3.68 **управление конфигурацией:** Порядок применения технической и административной директивы и контроля с целью определения и документирования функциональных и физических характеристик сложного устройства, управления изменением таких характеристик, ведения записей и отчетов об изменении в работе и настройке, а также проверки соответствия определенным требованиям (ГОСТ Р МЭК 61513).

3.69 **управляющие системы (элементы) безопасности**: Системы (элементы), предназначенные для инициирования действий систем безопасности, осуществления контроля и управления ими в процессе выполнения заданных функций (НП-001).

3.70 **управляющие системы, важные для безопасности АС:** Управляющие системы, представляющие совокупность управляющих систем безопасности и управляющих систем нормальной эксплуатации, важных для безопасности АС (РБ-004).

3.71 **управляющие системы (элементы) нормальной эксплуатации**: Системы (элементы), предназначенные для инициирования действий систем нормальной эксплуатации, осуществления контроля и управления ими в процессе выполнения заданных функций (НП-001).

3.72 **условия безопасной эксплуатации**: Установленные проектом АС минимальные требования по количеству, характеристикам, состоянию работоспособности, объему, периодичности и иным условиям технического обслуживания, контроля и испытаний систем (элементов), важных для безопасности, при которых обеспечивается соблюдение пределов безопасной эксплуатации и (или) критериев безопасности (НП-001).

3.73 **функция безопасности**: Конкретная цель и действия, обеспечивающие ее достижение, направленные на предотвращение аварий и (или) ограничение их последствий (НП-001).

3.74 **функциональное разнообразие:** Распространение разнообразия на функциональный уровень (например, активация останова как по предельной температуре, так и по предельному давлению) (ГОСТ Р МЭК 60880).

3.75 **функциональность:** Характеристика функции, которая определяет процедуры переработки входной информации в выходную информацию (ГОСТ Р МЭК 61513).

3.76 **функция, важная для безопасности:** Особая цель, которая должна способствовать безопасности (ГОСТ Р МЭК 61513).

3.77 **функция контроля и управления:** Функция контроля, управления и/или наблюдения за определенной частью процесса (ГОСТ Р МЭК 61513).

3.78 **цифровое устройство:** Устройство, реализация которого основана на операциях, выполняемых с помощью сигналов с определенными, дискретными уровнями, или в котором присутствуют определенные дискретные внутренние состояния и происходят переключения между этими состояниями.

Примечания

1 Функции таких устройств обычно определяются процессами, которые включают в себя разработку и испытание с применением языков описания программного обеспечения или аппаратуры; такие устройства могут внутренне управляться программным обеспечением или могут состоять из специализированных интегральных схем или FPGA и т.д., сконфигурированных с помощью программного обеспечения.

2 Устройства, оборудование или системы, которые управляются программным обеспечением, описывают как «компьютерные», тогда как «цифровой» является более широким термином, который охватывает любое устройство, использующее цифровые схемы для реализации логики.

3 Цифровые устройства, разработанные для неядерной промышленности, называют промышленными цифровыми устройствами.

3.79 **человеко-машинный интерфейс:** Интерфейс между оперативным персоналом, системой контроля и управления и информационно-вычислительными системами, обеспечивающими связь с АС. Данный интерфейс включает в себя СОИ, ОУ и интерфейс системы поддержки оператора (ГОСТ Р МЭК 60964).

3.80 **эксплуатация АС (эксплуатация)**: Вся деятельность, направленная на достижение безопасным образом цели, для которой была сооружена АС, включая

работу на мощности, пуски, остановы, испытания, техническое обслуживание, ремонт, перегрузку топлива, инспектирование во время эксплуатации и другую связанную с этим деятельность (НП-001).

3.81 **энергоблок:** Часть АС, выполняющая функцию АС в определенном проектом объеме.

3.82 **эргономическое обеспечение:** Установление эргономических требований и формирование эргономических свойств системы «человек-машина» на стадиях ее разработки и использования.

4 Сокращения

В настоящем стандарте применены следующие сокращения:

АВР - автоматическое включение резервов

АЗ - аварийная защита

АКНП - аппаратура контроля нейтронного потока

АРМ - автоматизированное рабочее место

АС - атомная станция

АСУ ТП - автоматизированная система управления технологическими процессами

БПУ - блочный пункт управления

ВС - вычислительные системы

ВОЛС - волоконно-оптические линии связи

ГИС - главный инженер станции

ГРП - группа руководства пуском

ЗИП - запасные инструменты и принадлежности

ЗПА - запроектная авария

ИПК - импульсный предохранительный клапан

ИБ - информационная безопасность

ИС - исходное событие

ИСКУ - интегрирующая система контроля и управления

ИФО - индивидуально функциональное опробование

КД - конструкторская документация

КИП - контрольно-измерительные приборы

МПУ - местные пункты управления

МПА - максимальная проектная авария

МРЗ - максимальное расчетное землетрясение

НКУ - низковольтное коммутирующее устройство

НСБ - начальник смены блока

НТД - нормативно-техническая документация

НЭ - нормальная эксплуатация

ОДУ - оперативно-диспетчерское управление

ОУ - органы управления

ОРД - организационно-распорядительный документ

ПЗ - предупредительная защита

ПИП - первичные измерительные преобразователи

ПМ - программы и методики

ПНР - пуско-наладочные работы

ПОС - проект организации строительства

ППР - проект производства работ

ПС - программное средство

ПТК - программно-технический комплекс

ПТС - программно-технические средства

ПК - приемочная комиссия

РД - руководящий документ

РПО - рабочее программное обеспечение

РПУ - резервный пункт управления

РС - рабочая станция

РУ - реакторная установка

САР - система автоматического регулирования

СБ - система безопасности

СВБ - система, важная для безопасности

СВРК	- система внутриреакторного контроля
СКУ	- система контроля и управления
СНЭ	- система нормальной эксплуатации
СОИ	- средства отображения информации
СПНИ	- система пусконаладочных измерений
СУЗ	- система управления и защит реакторной установки
СЗИ	- средства защиты информации
ТЗ	- техническое задание
ТЗБиС	- технологические защиты, блокировки и сигнализация
ТО	- техническое обслуживание
ТОУ	- технологический объект управления
ТП	- технический проект
ТПО	- тестовое программное обеспечение
ТРБЭ	- технологический регламент безопасной эксплуатации энергоблока
ТС	- техническое средство
ТУ	- технические условия
УПЗ	- ускоренная предупредительная защита
УС	- управляющая система
УСБ	- управляющая система безопасности
УСВБ	- управляющая система, важная для безопасности
УСНЭ ВБ	- управляющая система нормальной эксплуатации, важная для безопасности
ХГА	- хим-газовый анализ
ЧМИ	- человеко-машинный интерфейс
ЭБ	- энергоблок АС
ЭВМ	- электронно-вычислительная машина
ЭД	- эксплуатационная документация

5 Проектирование управляющих систем, важных для безопасности

УСВБ могут быть построены на оборудовании с использованием цифровых устройств, которые внутренне могут управляться программным обеспечением или могут состоять из специализированных интегральных схем или FPGA и т.д., сконфигурированных с помощью программного обеспечения.

В настоящем разделе приведены общие требования и рекомендации для проектирования архитектуры УСВБ, которые могут быть построены с использованием указанных технологий, и описана концепция жизненного цикла в целом для всей архитектуры системы контроля и управления энергоблока АС.

В действующих нормативных документах, относящихся к УСВБ, придается большое значение полноте и точности требований, вытекающих из целей, связанных с безопасностью АС. Эти цели являются исходными данными для выработки всесторонних требований к полной архитектуре СКУ энергоблока АС в целом, а также к отдельным УСВБ.

5.1 Основные требования к управляющим системам важным для безопасности

5.1.1 Требования по безопасности, которым должны соответствовать УСВБ энергоблока включают:

– концепцию управления энергоблоком и АС в целом;

– общие требования к функциям, системам и оборудованию контроля и управления энергоблока, важным для безопасности, исходя из анализа безопасности АС;

– требования к общей архитектуре СКУ энергоблока и АС, исходя из общих требований к функциям, системам и оборудованию контроля и управления;

– связи между требованиями архитектуры контроля и управления энергоблока и требованиями к отдельным УСВБ.

Для подтверждения того, что все требования по безопасности, которым должна соответствовать УСВБ, учтены и выполнены, используется системный подход. Это достигается путем проведения всей деятельности, связанной с проектированием,

разработкой, вводом в эксплуатацию, эксплуатацией и выводом из эксплуатации УСВБ, на основе использования идеологии полного жизненного цикла СКУ.

Фазы полного жизненного цикла контроля и управления энергоблоком при проектировании охватывают:

– разработку концепции управления энергоблоком АС;

– формирование основных требований к контролю и управлению энергоблоком на основе технологического задания, в том числе:

а) требований к функциональным и эксплуатационным характеристикам, а также независимости функций контроля и управления, важных для безопасности;

б) требований к функциям, выполняемым управляющими системами энергоблока;

в) особенностей проекта, характерных для конкретной АС;

– определение общей спецификации требований к функциям, системам и оборудованию контроля и управления энергоблоком;

– разработку полной архитектуры и распределение функций контроля и управления по отдельным управляющим системам и/или функциональным группам;

– разработку отдельных управляющих систем;

– общую интеграцию и приемку управляющих систем;

– эксплуатацию и обслуживание управляющих систем;

– модернизацию управляющих систем;

– вывод из эксплуатации управляющих систем.

5.1.2 Для создания исходных условий для проектирования общей архитектуры контроля и управления, вытекающих из анализа безопасности АС, должны быть установлены (специфицированы) исходные требования для функций, систем и оборудования энергоблока.

5.1.3 Требования к функциональным, эксплуатационным характеристикам, независимости для функций контроля и управления энергоблоком, важных для безопасности, и принципы эксплуатации энергоблока АС определяются в техническом задании и являются неотъемлемой частью всего проекта контроля и управления энергоблока и АС.

Основные положения технического задания должны содержать следующие исходные данные:

– концепцию глубокоэшелонированной защиты и группу функций, предназначенных для подавления последствий исходных событий;

– требования к характеристикам функций, важных для безопасности, которые должны отвечать общим требованиям обеспечения безопасности АС;

– требования к функциям автоматики и действиям оператора при управлении предусматриваемыми отклонениями от режимов нормальной эксплуатации и в условиях аварии;

– анализ задач, определяющий, какие функции должны быть переданы оператору, а какие – автоматике;

– перечень параметров технологического процесса, которые должны быть представлены оператору для выполнения им действий вручную;

– принципы приоритетности между действиями, выполняемыми автоматически и вручную оператором, с учетом категории функций.

В техническом задании должны быть отражены требования, вытекающие из данных общих технических требований.

5.1.4 Особенности проекта АС накладывают определенные ограничения на разработку архитектуры СКУ.

Проект СКУ энергоблока АС должен учитывать ограничения, накладываемые на оборудование контроля и управления особенностями проекта энергоблока АС, условиями взаимодействия управляющих систем с технологическим оборудованием, включая:

– границы между управляющими системами и технологическими системами АС, включая взаимодействие с исполнительными механизмами, а также устройствами энергоснабжения;

– диапазон условий окружающей среды в нормальных условиях эксплуатации, при отклонении от нормальных условий, а также в условиях учитываемых в проекте аварий, при которых должны работать управляющие системы;

– основные требования по размещению и прокладке кабелей;

– требования по электропитанию и заземлению;

– требования по стойкости оборудования к сейсмическим воздействиям;

– требования по ЭМС;

– требования по метрологическому обеспечению;

– требования по пожаробезопасности;

– требования по молниезащите;

Проект СКУ энергоблока АС, кроме того, должен учитывать эксплуатационные ограничения, накладываемые на оборудование контлроля и управления в части:

– требований по защите информации;

– требований по физической защите, а также защите от несанкционированного доступа к оборудованию / шкафам / панелям и т.д.;

– эксплуатации, технического обслуживания и ремонта;

– гарантийного обслуживания.

5.1.5 Общие спецификации требований к системам и оборудованию контроля и управления должны представлять совокупность спецификаций требований к каждой функции системы и ее оборудованию, важным для безопасности.

Общие спецификации требований должны охватывать все функции контроля и управления энергоблока в целом, начиная с входных устройств (датчиков, устройств обработки, другого оборудования) и заканчивая выходными (блоками управления исполнительными механизмами и другим оборудованием).

Общие спецификации требований должны включать:

– спецификацию требований к функциональности, определяющую, каким образом функция преобразует входную информацию в выходную с целью управления или контроля работы энергоблока АС;

– спецификацию требований к рабочим характеристикам, определяющую диапазон, точность и динамические характеристики функции и т.д;

– категории функции.

– требования к комбинации функций при их распределении по конкретным системам контроля и управления, включая:

а) комбинации функций, предназначенных для управления защитными действиями;

б) комбинации функций, обеспечивающих выполнения принципа глубокоэшелонированной защиты;

в) комбинации функций безопасности.

5.2 Разработка архитектуры СКУ энергоблока АС

5.2.1 Входной документацией при разработке полной архитектуры СКУ энергоблока являются:

– общая спецификация требований к функциям, системам и оборудованию контроля и управления, важным для безопасности;

– ограничения на разработку полной архитектуры СКУ энергоблока, накладываемые особенностями проекта АС.

Архитектура СКУ должна учитывать все аспекты контроля и управления, чтобы:

– выделить функции контроля и управления, важные для безопасности;

– распределить все проектные функции по отдельным частям СКУ и/или функциональным группам, с целью удовлетворения требований по:

а) разделению по классам безопасности;

б) выполнению требований, в том числе, по независимости, физическому разделению оборудования СКУ, ЭМС, квалификации, пожаробезопасности, молниезащите, метрологии, эксплуатационным ограничениям и т.д;

– предусматривать достаточное количество систем и подсистем (количество комплектов и каналов) для удовлетворения принципу единичного отказа;

– интерфейсы и взаимосвязи между управляющими системами были определены в составе проекта архитектуры, чтобы установить:

а) распределение технологических данных (измеренных параметров), необходимых для реализации всех функций, важных для безопасности;

б) выбор и приоритетность инициирующих и исполнительных сигналов различных систем;

в) пути прохождения сигналов и оборудование, которое является общим для выполнения автоматических функций и ручного управления на различных уровнях глубокоэшелонированной защиты.

5.2.2 Архитектура СКУ энергоблока АС должна распределить системы с элементами человеко-машинного интерфейса (ЧМИ) по различным помещениям АС, предназначенным для управления и контроля технологического процесса (БПУ, РПУ, МПУ/МЩУ) с необходимой степенью резервирования и с учетом эксплуатационных ограничений.

В архитектуре СКУ должны быть определены:

– принципы приоритетности между автоматическим и ручным управлением технологическим оборудованием энергоблока;

– принципы приоритетности между различными системами с элементами ЧМИ при нормальной эксплуатации, при авариях и при послеаварийных режимах эксплуатации;

– принципы приоритетности между основным и резервным оборудованием с элементами ЧМИ;

– принципы получения оператором информации о сбоях и отказах технологического оборудования и оборудования СКУ, при этом форма представления информации должна позволять оператору:

а) быстро опознать и идентифицировать отказ по индикации;

б) принять решение о применении ручного управления для перевода энергоблока в безопасное состояние;

в) идентифицировать систему (оборудование системы), которое необходимо восстановить;

– функции, выполняемые автоматически и вручную оператором в соответствии с анализом задач;

– способность СКУ осуществить необходимую обработку информации и выполнить задачи, определенные в результате взаимодействия с оператором энергоблока;

– объем необходимой информации для оператора энергоблока и время, необходимое для выполнения управления энергоблоком вручную.

При разработке ЧМИ должны быть рассмотрены задачи оператора и оптимизированы требования к взаимодействию человек-машина при выполнении задач, как важных для безопасности, так и не влияющих на безопасность.

5.2.3 Средства передачи данных между управляющими системами, образующими архитектуру СКУ энергоблока и АС должны:

– удовлетворять общей спецификации требований к рабочим характеристикам при всех условиях и режимах работы энергоблока и АС в целом;

– обеспечить соблюдение требований независимости систем;

– включать средства проверки работоспособности коммуникационного оборудования и полноты передаваемых данных;

– обеспечивать резервирование линий передачи данных;

– обеспечивать отсутствие взаимного влияния выполнения разных функций при передаче данных.

5.2.4 Меры защиты от отказов по общей причине включают:

– проектные решения по обеспечению устойчивости к внутренним и внешним воздействиям, которые могут привести к отказу по общей причине, в том числе повреждение или полное уничтожение оборудования УСВБ (умышленно или при внешних воздействиях):

а) размещение резервных частей системы в различных помещениях;

б) независимость источников энергоснабжения для каналов и систем;

в) противопожарная защита, защита от воздействия химических веществ, вибрации и т. д;

г) проектирование оборудования в соответствии с ГОСТ и стандартами IEC по электромагнитной совместимости;

д) квалификация оборудования по воздействию окружающей среды и сейсмостойкости;

– проектные решения, направленные против отказов по общей причине вследствие отказов источников энергоснабжения и изменения качества электропитания;

– проектные решения по минимизации использования общих ресурсов в архитектуре контроля и управления для различных уровней защиты;

– использование разнообразия, в том числе:

а) функциональное разнообразие;

б) разнообразие проектных решений;

в) разнообразие программного обеспечения;

г) разнообразие оборудования;

– принятие проектных решений по ограничению сложности, в том числе ограничение сложности технических и программных средств.

5.2.5 Когда все функции (и требования к ним) для управляющих систем энергоблока определены, они распределяются по отдельным управляющим системам полной архитектуры СКУ. При таком распределении необходимо учитывать следующее:

– спецификация функциональных требований и требований к характеристикам прикладных функций должны учитываться в общих требованиях к функциям СКУ;

– спецификация функциональных требований и требований к характеристикам прикладных функций СКУ должны включать все функции, которые были определены при проектировании архитектуры СКУ;

– распределение прикладных функций по составным частям СКУ энергоблока или АС должно соответствовать классу систем по безопасности;

– по результатам распределения прикладных функций по составным частям СКУ необходимо оптимизировать сложность систем;

5.2.6 Выходная документация по архитектуре СКУ и распределению функций является источником необходимых исходных данных для технического задания на отдельные составные части СКУ энергоблока и АС в целом.

Выходная документация должна определять для каждой управляющей системы:

– ограничения, возникшие из-за особенностей АС;

– ограничения, связанные с архитектурой;

– физическое и функциональное разграничение между управляющими системами;

– функциональные требования, требования к характеристикам и надежности выполнения прикладных функций, назначенных каждой системе.

Требования могут быть оформлены в виде текстовой документации, блок-схем, структурных схем и пр., обеспечивающей ясное представление о функциях.

Спецификация требований к прикладным функциям не должна зависеть от характеристик применяемой технологии цифровых устройств.

Для разработки выходных документов должны использоваться инжиниринговые методы и инструментальные средства разработки систем и программного обеспечения.

Документация на используемый инжиниринговый инструментарий должна содержать информацию, из которой должно быть видно:

– каким образом проектирование (как фаза жизненного цикла системы) опирается на используемые инструментальные средства;

– как должно использоваться каждое инструментальное средство;

– как должна верифицироваться выходная информация каждого инструментального средства.

Требования к инжиниринговым методам и инструментальным средствам создания программного обеспечения для УСВБ даны в ГОСТ Р МЭК 60880.

6 Разработка управляющих систем, важных для безопасности

В общей архитектуре СКУ энергоблока и АС, разработанной на этапе проектирования, выделяются отдельные управляющие системы, которые выполняют функции, важные для безопасности. Настоящий раздел устанавливает требования к таким системам.

Данные требования охватывают свойства управляющих систем, относящиеся:

– к прикладным функциям, назначенным системе в процессе распределения функций;

– к основным характеристикам системы (оборудованию системы), которые в соответствии с системой классификации делают систему пригодной для выполнения функций, важных для безопасности, определенных проектом.

Фазы типичного жизненного цикла управляющих систем включают:

– разработку технического задания на систему;

– разработку технических заданий на технические и программные средства системы;

– технический проект на систему;

– рабочее проектирование и реализацию системы;

– интеграцию системы;

– валидацию системы;

– внедрение системы;

– модификацию проекта системы (при необходимости).

6.1 Этапы разработки

В таблице 1 представлены этапы разработки УСВБ.

Таблица 1 – Этапы разработки управляющих систем, важных для безопасности

<table>
<tr><td colspan="3">Спецификация требований к системе
ТЗ на систему
(Примечание 1, 2, 3)</td></tr>
<tr><td>ЧТЗ на ТС
(примечание 2)</td><td>ЧТЗ на ПО
(примечание 1, 3)</td><td>ЧТЗ на ПЧ для Полигона
(примечание 1, 2, 3)</td></tr>
<tr><td>Разработка КД
(примечание 2)</td><td>ТП на ПО
(примечание 1)</td><td>Изготовление и поставка ПЧ на Полигон
(примечание 1, 2, 3)</td></tr>
<tr><td>Изготовление
(примечание 2)</td><td>Кодирование
(примечание 1)</td><td>Испытания</td></tr>
<tr><td>Квалификация
(примечание 4)</td><td></td><td></td></tr>
<tr><td colspan="3">Интеграция
(примечание 1)</td></tr>
<tr><td colspan="3">Приемосдаточные испытания</td></tr>
<tr><td colspan="3">Предварительные автономные испытания (1этап)</td></tr>
<tr><td colspan="3">Примечания
1 Требования к программному обеспечению на данной стадии определены в ГОСТ Р МЭК 60880.
2 Требования к оборудованию на данной стадии определены в IEC 60987 [7].
3 Требования к существующему программному обеспечению на данной стадии определены в ГОСТ Р МЭК 60880.
4 Требования к квалификации оборудования на данной стадии определены в IEC/IEEE 60780-323 [1].</td></tr>
</table>

6.2 Техническое задание на систему

6.2.1 Выходная документация технического проекта СКУ энергоблока и АС в целом, описывающая общую архитектуру контроля и управления и распределение функций по отдельным управляющим системам, является исходной для создания технического задания на систему (ТЗ на систему).

6.2.2 Техническое задание на УСВБ – это описание требований к объединенной системе комплекса технических и программных средств с указанием целей и функций системы.

6.2.3 В ТЗ на систему описываются все характеристики системы, ее функции, цели и ограничения, которые должны быть учтены при ее разработке. Эти сведения должны:

– быть сформулированы с использованием точных терминов и измеряемых величин;

– быть последовательными и не содержать никаких противоречивых требований;

– являться отслеживаемыми (т.е. источник основных требований должен быть известен).

6.2.4 ТЗ на систему должно определять следующие требования:

1) функциональные характеристики системы, в том числе:

– прикладные функции;

– сервисные функции;

– программные средства;

– алгоритмические преобразования между входами и выходами системы, как при нормальном режиме работы, так и при деградации системы;

– входы системы, а именно: источник сигнала, параметры сигнала, диапазон изменений, диапазон достоверности и т.д.;

– обработку данных, а именно: проверку достоверности входных данных, последовательность операций, отклик на ненормальную ситуацию, проверку достоверности выходных данных и т.д.;

– выходы системы, а именно: получателя сигнала, параметры выходного сигнала, динамические характеристики, диапазон достоверности, сообщение об ошибках системы;

– основные функции прикладного языка (если это необходимо);

– поведение системы при запуске, повторном запуске;

2) требования по эксплуатационным характеристикам системы, в том числе:

– количество операций, выполняемых системой за данное время при нормальных и ограничивающих условиях (например, при деградации системы);

– выполняемые операции;

– объемы потоков данных с внешними устройствами;

– способность системы к распознаванию событий;

– время отклика системы;

– разрешающая способность синхронизации по времени;

– число пользователей системы;

3) проектные ограничения, в том числе:

– проектные ограничения, обусловленные классификацией прикладных функций и концепцией защиты в глубину;

– детерминированное поведение подсистемы;

– требования к техническому диагностированию;

– ремонтопригодность;

– исключение несанкционированного доступа и возможности ложного обесточивания оборудования;

– обеспечение контроля на БПУ состояния всех источников питания;

– обеспечение представления информации на БПУ о состоянии каналов СБ;

– характеристики эксплуатационной безопасности, в том числе:

а) эксплуатационная надежность;

б) эксплуатационная готовность;

в) время восстановления системы;

4) удобство эксплуатации, в том числе:

– требования по удобству эксплуатации технических и программных средств, входящих в состав системы, в том числе наличие необходимых средств документирования;

– ресурсы, необходимые при выполнении модификаций на этапе эксплуатации системы;

– другие характеристики, такие как:

а) переносимость программных средств;

б) соответствие принятым нормативным документам и стандартам;

5) средства проверки работоспособности, в том числе:

– основные тесты, используемые системой в заводских условиях и на АС, чтобы проверить правильность работы с функциональной точки зрения;

– необходимые ресурсы системы для проведения тестирования;

– продолжительность периода и условия отслеживания поведения оборудования интегрированной системы при эксплуатации;

6) документацию, которая должна быть выпущена вместе с системой:

– при разработке технических и программных средств;

– при поставке на АС вместе с системой (исходные тексты программ, руководство системного программиста (системного администратора, администратора ИБ), руководство оператора, руководства по эксплуатации технических средств, входящих в состав системы, паспорта на технические средства системы, руководство по эксплуатации системы, формуляр на систему и т.д.);

7) границы системы и связи с другими системами:

– физические ограничения, связанные с размещением системы;

– физические и функциональные интерфейсы со смежными системами (способ соединения, протоколы связи, тип передаваемой и получаемой информации);

8) ожидаемые функции интерфейса «человек-машина» для разных пользователей системы (операторов, ремонтного персонала, системных администраторов, администраторов баз данных);

9) условия окружающей среды в предельных условиях эксплуатации;

10) требуемую квалификацию оборудования;

11) техническое задание на УСВБ является основным документом, определяющим требования и порядок создания системы. Состав, содержание, оформление, а также порядок разработки, согласования и утверждения ТЗ должно соответствовать ГОСТ 34.602 и требованиям настоящего документа.

6.3 Требования к функциям системы

6.3.1 Прикладные функции

6.3.1.1 Спецификация требований к каждой прикладной функции должна устанавливать:

– функциональность, включая диапазоны входных и выходных сигналов и уставки;

– рабочие характеристики, включающие точность и время отклика, при этом требования к рабочим характеристикам определяют для всех возможных исходных условий на АС и проектных исходных событий;

– категорию функции (функция безопасности, важная для безопасности, не влияющая на безопасность);

– ограничения со стороны других функций безопасности, если эти ограничения существуют.

6.3.1.2 При распределении функций СКУ энергоблока по конкретным управляющим системам для каждой категории функций должен быть определен минимальный класс ФГ и системы.

6.3.1.3 Вместе с требованиями к независимости функций системы (критерий единичного отказа, проектная защита от отказа по общей причине и т.д.), такие факторы позволяют выполнить качественную оценку надежности функции или ряда функций системы.

6.3.1.4 Количественная оценка надежности прикладных функций должна выполняться при разработке оборудования системы.

6.3.1.5 Количественная оценка надежности программных средств может не выполняться, так как в настоящее время не существует методов, пригодных для такой объективной оценки.

6.3.2 Сервисные функции

6.3.2.1 Сервисные функции управляющей системы напрямую не связаны с выполнением действий, связанных с технологическим процессом и включают в свой состав функции, необходимые для конфигурирования системы, испытаний, эксплуатации, периодических испытаний, обслуживания, ведения модификаций и т.д.

6.3.2.2 Спецификацию требований к сервисным функциям управляющей системы определяются ее разработчиком и, как правило, окончательно могут быть сформулированы только на фазе разработки архитектуры системы.

6.3.3 Требования к программным средствам

6.3.3.1 Техническое задание на УСВБ должно давать полное представление о функциях, выполняемых ПС.

6.3.3.2 Требования к ПС определяются требованиями к прикладным функциям и проектными ограничениями на систему, представляют собой часть

функциональных требований закрепленных за системой и должны быть полностью определены как для вновь разрабатываемых программных средств, так и апробированных (ранее разработанных).

6.3.4 Проектные ограничения

6.3.4.1 Приведенные ниже требования к УСВБ в основном определяют проектные ограничения, которые ограничивают выбор технических решений при задании функций системе и ее проектировании.

6.3.4.2 Ограничения для УСВБ зависят от категорий заданных ей функций и должны учитываться при разработке спецификации системы и ее архитектуры для того, чтобы:

– выполнить требования, обусловленные категорией прикладных функций;

– обеспечить функционирование системы в соответствии с проектом;

– обеспечить возможность демонстрации правильности работы системы.

6.3.5 Архитектура системы

6.3.5.1 Архитектура системы определяется категориями функций, которые должны выполняться системой, и принятой концепцией глубоко эшелонированной защиты.

6.3.5.2 Система может обеспечивать выполнение функции разных категорий (функций безопасности, функций, не влияющих на безопасность) и включать в свой состав ФГ разных классов безопасности. При этом должно обеспечиваться выполнение следующих требований:

– проектные требования к каждой ФГ системы должны соответствовать категории функции, выполнение которой обеспечивает данная ФГ системы;

– проект системы должен обеспечивать выполнение требований по отсутствию влияния отказов ФГ и оборудования более низкого класса по безопасности на оборудование более высокого класса.

6.3.5.3 Проект системы должен предусматривать резервирование и другие свойства, необходимые для обеспечения устойчивости к отказу и поддержания прикладных функций, важных для безопасности.

6.3.5.4 Проект системы должен удовлетворять требованиям принципа независимости для того, чтобы:

– предохранить ее от влияния отказов систем с меньшим уровнем влияния на безопасность;

– предохранить ее от взаимного влияния отказов резервированных ветвей оборудования (если такое резервирование предусмотрено).

6.3.5.5 Проект УСВБ должен предусматривать достаточное резервирование, чтобы удовлетворять критерию единичного отказа для функций аварийных защит, как при эксплуатации, так и при обслуживании системы.

6.3.5.6 Следует отметить, что отказы программных средств (ПС) являются систематическими, а не случайными. По этой причине критерий единичного отказа не может применяться при разработке ПС системы в том виде, как это делается при проектировании оборудования. В этом случае для каждой системы и ее архитектуры следует рассматривать все возможные воздействия отказа по общей причине из-за ПС на каждом уровне защиты либо между резервированными каналами.

6.3.6 Внутреннее поведение системы

6.3.6.1 Проект управляющей системы должен обеспечивать детерминированное поведение, согласующееся с требованиями к характеристикам назначенных функций.

6.3.6.2 Управляющая система имеет детерминированное поведение, если временная задержка между воздействием и откликом имеет гарантированные минимум и максимум при всех проектных условиях эксплуатации.

6.3.6.3 Компьютерные сети должны быть спроектированы таким образом, чтобы удовлетворить требованиям к пропускной способности данных при всех режимах эксплуатации АС, включая ожидаемые переходные процессы и аварийные условия.

6.3.7 Требования к техническому диагностированию

6.3.7.1 Техническое диагностирование предусматривает:

– контроль технического состояния оборудования системы;

– обнаружение мест и определение причин возникновения дефектов;

– прогнозирование технического состояния.

6.3.7.2 Контроль технического состояния осуществляется путем сопоставления количественных и качественных характеристик оборудования системы, полученных на основании анализа реакций (выходных сигналов) на рабочие или специальные тестовые воздействия (тестовые входные сигналы), с допускаемыми характеристиками, которые определяют работоспособность и/или правильность функционирования системы.

6.3.7.3 Контроль технического состояния должен охватывать:

– компоненты системы;

– независимые резервированные каналы системы;

– цепи передачи сигналов и команд;

– линии связи и локальные сети.

6.3.7.4 Контроль технического состояния оборудования системы должен осуществляться:

– после включения электропитания;

– непрерывно в процессе работы;

– периодически.

6.3.7.5 После включения электропитания должны автоматически контролироваться:

– работоспособность оборудования при помощи встроенных проверяющих тестов;

– отсутствие искажений в программах и данных;

– соответствие состава и конфигурации системы проектным характеристикам;

– соответствие загруженной версии ПС фактическому составу и конфигурации системы;

– исправность цепей передачи сигналов и команд;

– правильность обмена сообщениями между составными частями системы по линиям связи и/или локальным сетям.

6.3.7.6 В процессе работы УСВБ должен осуществляться непрерывный автоматический контроль:

– наличия электропитания;

– исправности цепей передачи сигналов и команд, включая цепи дистанционного управления;

– достоверности аналоговых и дискретных входных сигналов;

– отсутствия ошибок при обмене данными между составными частями системы;

– отсутствия ошибок в данных, принимаемых от других систем или оборудования;

– отсутствия сбоев, вызвавших прекращение выполнения программы;

– правильности функционирования оборудования системы (при помощи встроенных средств непрерывного диагностирования);

– нарушения температурного режима работы оборудования системы;

– состояния средств технического диагностирования.

6.3.7.7 В случае обнаружения дефекта при контроле технического состояния после включения электропитания или в процессе работы, средства технического диагностирования в составе системы должны автоматически определять место и причину возникновения дефекта и выдавать тревожное сообщение персоналу.

6.3.7.8 Результаты технического диагностирования должны отображаться по вызову персонала в виде диагностических сообщений.

6.3.7.9 Диагностическое сообщение должно отображать состояние системы и/или оборудования системы и места возникновения дефектов, если они обнаружены.

6.3.7.10 Периодический контроль технического состояния должен охватывать:

– компоненты системы / оборудования системы, для которых не предусматривается непрерывный автоматический контроль технического состояния;

– средства технического диагностирования, осуществляющие контроль технического состояния после включения электропитания и в процессе работы.

6.3.7.11 В процессе периодического контроля технического состояния должна быть получена информация о действительных значениях выбранных диагностических признаков (точностных, метрологических, временных характеристиках и т.п.) и о тенденциях изменения диагностических признаков,

которые позволяют выявить ухудшение свойств и прогнозировать приближение постепенных отказов компонентов системы.

6.3.7.12 Условия проведения периодического контроля технического состояния должны сводить к минимуму возможность любого отрицательного воздействия на работу и состояние безопасности энергоблока.

6.3.7.13 В процессе периодического контроля технического состояния должна быть предусмотрена проверка работоспособности УСБ, а также систем, совмещающих функций УСБ и УСНЭ (УСВБ) для проверки правильности формирования команд защитных действий при имитации нарушений пределов и условий безопасной эксплуатации с помощью проверяющих тестов.

6.3.7.14 Для однокомплектной системы проверка работоспособности должна проводиться для каждого из независимых резервированных каналов в отдельности, при этом выходной сигнал проверяемого канала должен автоматически устанавливаться в сработанное состояние, соответствующее наличию исходного события, и удерживаться в этом состоянии до завершения проверки.

6.3.7.15 Не допускается проведение проверок:

– одновременно более чем одного независимого резервированного канала;

– любого независимого резервированного канала при обнаружении дефекта в каком-либо другом независимом резервированном канале;

– при выводе из работы любого из независимых резервированных каналов для технического обслуживания или восстановления.

6.3.7.16 Состав сервисного оборудования, необходимого для проведения периодического контроля технического состояния, указывают в ТЗ на систему, в ТЗ и/или ТУ на оборудование системы.

6.3.7.17 Сервисное оборудование должно подсоединяться без нарушения внешних связей оборудования системы.

6.3.7.18 Техническое диагностирование не должно влиять на выполнение основных функций системы и/или приводить к ухудшению ее характеристик.

6.3.7.19 Отказы компонентов, осуществляющих техническое диагностирование, не должны приводить к отказам основных информационных и управляющих функций системы.

6.3.7.20 Способ тестирования должен сводить к минимуму время, в течение которого цепь защиты выводится из штатной работы для тестирования.

6.3.8 Ремонтопригодность

6.3.8.1 Система должна быть спроектирована так, чтобы:

– была обеспечена возможность удобного обслуживания оборудования системы, его диагностики при отказе, безопасного ремонта или замены и калибровки;

– свести к минимуму риск и нагрузку на персонал при выполнении обслуживания и ремонта.

6.3.8.2 Проверке после обслуживания и ремонта подлежат:

– правильность восстановления соединений в цепи;

– правильность калибровки аналоговых каналов измерений и всех аварийных уставок;

– способность системы выполнять предусмотренные функции, важные для безопасности.

6.3.8.3 При разработке систем в части обслуживания, тестирования, а также ремонтопригодности необходимо руководствоваться:

– рекомендациями IEC 60987 [7] для УСВБ;

– требованиями NS-G-1.3 [2] для систем, выполняющих функции УСБ;

– требованиями NS-G-1.3 [2] для систем, связанных с обеспечением безопасности.

6.3.9 Интерфейсы с другими системами и техническими средствами

6.3.9.1 Чтобы обеспечить интеграцию системы в архитектуру контроля и управления, необходимо учитывать следующие факторы:

– физические ограничения, связанные с размещением системы в проектном помещении на АС;

– физические и функциональные интерфейсы системы с обслуживающими системами и оборудованием;

– физические и функциональные интерфейсы системы с вспомогательными системами и оборудованием, с которыми она обменивается информацией;

– интерфейсы с программными инструментальными средствами, используемыми для обеспечения обмена данными между системами и проверки достоверности этих данных.

6.3.9.2 Требования, которым должны удовлетворять каналы передачи данных ТС / ПТС / ПТК управляющих систем энергоблока, должны быть изложены в отдельном документе, который должен быть разработан в развитие настоящего документа.

6.3.10 Интерфейсы пользователей

Требования к ЧМИ должны обеспечивать минимальный риск ошибки персонала, например, неумышленной ошибки, недосмотра, пропуска информации при пуске, эксплуатации, тестировании и обслуживании системы.

6.3.11 Условия окружающей среды

6.3.11.1 В соответствии с ограничениями, накладываемыми со стороны проекта АС, следует определить диапазоны нормальных и аварийных условий внешней среды, при которых система должна сохранять работоспособность.

6.3.11.2 Перечни учитываемых условий окружающей среды должны содержать:

– температуру при нормальной эксплуатации и в условиях аварий;

– влажность при нормальной эксплуатации и в условиях аварий;

– давление при нормальной эксплуатации и в условиях аварий;

– уровень радиации при нормальной эксплуатации и в условиях аварий;

– уровень электромагнитных помех при нормальной эксплуатации и в условиях аварий;

– возможные опасные воздействия, внешние по отношению к системе, включая сейсмические;

– время воздействия предельных условий окружающей среды при авариях;

– условия энергоснабжения и отвода тепла.

6.3.11.3 При этом в соответствии с ОТТ 08042462 определяются:

– факторы внешней среды и время их воздействия для разных групп размещения при нормальной эксплуатации и в условиях аварий;

– требования к устойчивости к вибрациям и сейсмическим воздействиям;

– требования по пожаробезопасности;

– требования по надежности, средней наработке на отказ,

– требования к электропитанию систем контроля и управления, важных для безопасности (с учетом рекомендаций ГОСТ Р МЭК 61225);

6.3.11.4 Внешние условия, связанные с электромагнитными помехами, определяются в соответствии с ГОСТ 32137;

6.4 Разработка технических средств системы

6.4.1 Разработка технических средств УСВБ включает следующие этапы:

– разработку ТЗ на технические средства в соответствии с техническим заданием на управляющую систему;

– разработка КД на технические средства системы;

– изготовление опытных образцов технических средств системы;

– проведение квалификационных испытаний опытных образцов;

– корректировка КД по результатам квалификационных испытаний опытных образцов оборудования и полигонных испытаний представительных частей системы;

– разработка качественного и количественного анализа надежности ТС системы;

– присвоение КД на оборудование литеры О (О1);

– изготовление поставочного комплекта оборудования системы;

– интеграция технических и программных средств системы;

– приемосдаточные испытания поставочного комплекта оборудования системы;

6.4.2 Разработка ПТС управляющих систем, важных для безопасности и постановка ее на производство должна соответствовать требованиям ГОСТ Р 15.301 и рекомендациям IEC 60987 [7].

6.4.3 Испытания и приемка ПТС управляющих систем, важных для безопасности должна соответствовать требованиям ГОСТ 15.309.

6.4.4 Правила построения, изложения, оформления, согласования и утверждения технических условий на ПТС управляющих систем должны соответствовать требованиям ГОСТ 2.114.

6.4.5 Виды, комплектность и правила выполнения эксплуатационной документации на ПТС управляющих систем, должны соответствовать требованиям ГОСТ 2.601.

6.4.6 Эксплуатационная документация на ПТС управляющих систем должна быть согласована с Заказчиком управляющей системы до присвоения КД на оборудование литеры О (О1).

6.4.7 Качество изготовления оборудования должно обеспечиваться системой качества, действующей на предприятии-изготовителе.

6.4.8 В случае применения при разработке и изготовлении ПТС УСВБ изделий, материалов и комплектующих зарубежных поставщиков, условия поставки должны соответствовать НП-071.

6.4.9 Условия поставки определяют процедуру оценки соответствия импортного оборудования и изделий, влияющих на безопасность ядерных установок, а также импортных материалов и комплектующих, в том числе непосредственно поставляемых на объекты использования атомной энергии, требованиям действующих в Российской Федерации норм и правил в области использования атомной энергии.

6.4.10 Обязательными условиями применения импортного оборудования, изделий, материалов и комплектующих являются:

– соблюдение законодательства России в области использования атомной энергии;

– соблюдение требований норм, правил и других нормативных документов России в области использования атомной энергии;

– соблюдение требований обязательной сертификации, установленных Системой сертификации оборудования, изделий и технологий для ядерных установок, радиационных источников и пунктов хранения;

– наличие положительного опыта применения импортного оборудования, изделий, материалов и комплектующих на объектах использования атомной энергии зарубежных стран;

– исключение ухудшения предусмотренных проектом объекта использования атомной энергии характеристик (параметров) оборудования и систем, в которых предполагается использование импортного оборудования, изделий и комплектующих, а также негативного воздействия на выполнение функций других систем объектов использования атомной энергии;

– наличие возможности проведения Заказчиком и надзорным органом контрольных проверок и оценок качества оборудования, изделий, материалов и комплектующих в процессе изготовления и/или, в отдельных случаях, после изготовления (если оборудование, изделия, материалы и комплектующие были изготовлены к моменту заключения контракта на поставку), а также испытаний у Поставщика.

6.4.11 Перед заключением Договора на поставку Заказчиком оборудования, изделий, материалов, комплектующих должен провести предварительную оценку возможности поставки, при этом процедура предварительной оценки должна соответствовать требованиям НП-071.

6.4.12 Требования к содержанию, порядку оформления и согласования Решений о применении импортной продукции на действующих и строящихся АЭС определены в РД ЭО 1.1.2.01.0958.

6.5 Разработка программных средств системы

6.5.1 Общие требования к программным средствам

6.5.1.1 Конфигурация ПТС системы должна определяться функциональными требованиями к СКУ, а также требованиями надежности и среды функционирования. Техническое задание на СКУ должно давать полное представление о функциях, выполняемых ПС.

6.5.1.2 Требования к ПС вытекают из требований к СКУ и являются их частью.

6.5.1.3 Функциональные требования к ПС должны представлять собой часть функциональных требований, которые закреплены за системой и которые должны быть этой системой реализованы.

6.5.1.4 Требования к надежности ПС представляют собой расширение требований к надежности системы и должны быть введены в состав требований к ПС аналогично функциональным требованиям.

6.5.1.5 ПС должны проектироваться в соответствии с принципами структурного или объектно-ориентированного программирования. ПС, как правило, должны выполняться в виде законченных модулей законченного смыслового характера (один модуль - одна функция).

6.5.1.6 Текст модуля должен содержать, как правило, не более 100 операторов исходного языка.

6.5.1.7 Конфигурация УСВБ должна предусматривать возможность периодического тестирования (проверок, опробований, испытаний) системы, например, во время останова энергоблока АС, при этом тестированию должна подвергаться каждая функция системы.

6.5.1.8 Конфигурация системы должна предусматривать возможность ее самопроверки. Самопроверка не должна увеличивать время задержки реакции системы на внешние воздействия выше допускаемых пределов, а также негативно влиять на обеспечение безопасности АС.

6.5.1.9 ПС вычислительной системы должно быть разделены таким образом, чтобы программы, обслуживающие оператора, были отделены от прикладных программ.

6.5.1.10 Программы различного функционального назначения должны быть защищены от возможных взаимных искажений при сбоях и ошибках.

6.5.1.11 При разработке УСВБ следует отдавать предпочтение использованию готовых и апробированных программных средств (операционные системы, СУБД и др.).

6.5.1.12 В ПС УСВБ должны быть предусмотрены:

– средства защиты от искажений входной информации, поступающей от измерительных средств и по каналам связи от смежных систем;

– средства защиты от сбоев и частичных отказов вычислительных средств системы, в том числе по общей причине;

– средства, предотвращающие несанкционированный доступ к программным кодам и информации;

– средства защиты прикладных программ и информации от ошибочных действий персонала;

– средства подтверждения операторского запроса на вмешательство в работу программ, влияющих на безопасность;

– средства защиты от искажений информации в аварийных режимах работы энергоблока;

– средства тестирования и самопроверки.

6.5.1.13 Программное и информационное обеспечение УСВБ должно строиться на единой системе программных средств (программных библиотек), иметь единую структуру и организацию данных, снабжаться встроенными программными средствами информационно-справочной поддержки персонала и соответствующей программной документацией.

6.5.1.14 В процессе разработки ТС должно быть обеспечено их соответствие показателям качества по факторам, установленным ГОСТ 28195 (сопровождение, удобство применения, эффективность, универсальность и корректность).

6.5.2 Этапы разработки программных средств

6.5.2.1 Применительно к УСВБ этапы выполнения проекта ПС должны быть формализованы, причем в ходе выполнения проекта не допускается исключать ни один из этапов.

6.5.2.2 Мероприятия по обеспечению качества должны выполняться на всех этапах жизненного цикла ПС, начиная с этапа разработки технического задания на систему, до стадии ввода ее в эксплуатацию. Каждый этап жизненного цикла ПС должен быть формально определен и оформлен соответствующей документацией.

6.5.2.3 Жизненный цикл УСВБ включает следующие основные стадии создания ПС:

– разработку ТЗ на систему;

– разработку ТЗ на ПС;

– разработку проекта ПС, в том числе:

а) технический проект;

б) рабочий проект;

– рабочее программирование ПС;

– интеграцию системы;

– тестирование интегрированной системы;

– комплексные испытания системы;

– ввод управляющей системы в эксплуатацию на объекте.

6.5.2.4 В случае использования ранее разработанных (апробированных) ПС при создании УСВБ жизненный цикл разработки ПС может иметь некоторые особенности, связанные с использованием ранее разработанных ПС и включает следующие основные этапы его создания:

– разработку ТЗ на систему;

– разработку ТЗ на ПС;

– разработку проекта ПС, в том числе:

а) технический проект;

б) рабочий проект;

– оценку соответствия ранее разработанных ПС проектным требованиям;

– приобретение (закупка) ранее разработанных ПС;

– рабочее программирование;

– интеграцию системы;

– тестирование интегрированной системы;

– комплексные испытания системы;

– ввод управляющей системы в эксплуатацию на объекте.

6.5.3 Планирование проекта создания программных средств

6.5.3.1 Каждый этап разработки ПС должен быть документально оформлен.

6.5.3.2 Каждый из этапов жизненного цикла ПС должен быть разделен на отдельные элементарные задачи и объем работ по задачам должен быть четко определен.

6.5.3.3 После завершения работ по каждому из этапов должна быть выполнена проверка всех компонентов ПС.

6.5.3.4 Каждый этап разработки ПС должен завершаться верификацией результатов.

6.5.3.5 Успешное завершение верификации является основанием для начала следующей стадии.

6.5.3.6 Систематическое выполнение критического анализа составляет главную часть процесса верификации этапов проектирования ПС.

6.5.3.7 Верификация результатов каждого этапа должна завершаться отчетом с результатами проведенного анализа, составленными заключениями и согласованными решениями. Каждый отчет необходимо включить в состав проектной документации.

6.5.3.8 В зависимости от специфики и класса безопасности разрабатываемых ПС, Разработчик УСВБ должен разработать собственные процедуры на основании положений и рекомендаций, изложенных в нормативных документах (ГОСТ Р МЭК 60880, IEEE Std 1012 [3], ANSI/ANS-10.4-2008 [4]).

Разработанные процедуры должны быть согласованы с Заказчиком УСВБ.

Состав и содержание документации, разрабатываемой на каждом этапе жизненного цикла ПС, должны соответствовать требованиям нормативных документов, должны быть определены в собственных процедурах организации-разработчика и согласованы с Заказчиком.

6.5.4 Классификация программных средств

6.5.4.1 Классы безопасности УСВБ назначаются разработчиками проекта реакторной установки и разработчиками проекта атомной станции в соответствии с НП-001.

6.5.4.2 Программные средства, используемые в УСВБ, классифицируется согласно классу безопасности ФГ, которые используют эти ПС.

6.5.5 Техническое задание на Программное средство

6.5.5.1 Техническое задание на ПС должно быть разработано с учетом требований, предъявляемых к системам, важным для безопасности АС, и являются частью Технического задания на систему.

6.5.5.2 Техническое задание на ПС должно быть подготовлено до начала реализации этапа проектирования и программирования. Документ должен быть полным, последовательным, выполненным на уровне современных требований к ПС. Требования должны быть недвусмысленными, поддающимися испытаниям или проверке.

6.5.5.3 Техническое задание на ПС должно содержать:

– требования к системе;

– требования к функционированию системы во всех проектных режимах работы энергоблока;

– требования к загруженности системы во всех проектных режимах работы энергоблока;

– архитектуру системы;

– требования к человеко-машинному интерфейсу;

– требования к внутренним и внешним интерфейсам;

– описание функций системы;

– структуру и взаимосвязь данных;

– описание разграничения функций между техническими и ПС системы;

– описание специальных условий эксплуатации;

– требования к самоконтролю системы.

6.5.6 Технический проект

На этапе технического проекта:

– должно быть обеспечено решение требований по обработке данных, точно описанных в спецификациях на ПС;

– должна быть определена архитектура ПС, разбитая на блочную (модульную) структуру;

– должна быть определена организация блочной структуры (последовательность обработки, обмен данными, вызовы и т.д.);

– должны быть определены взаимосвязи каждого программного блока, при этом каждый блок должен иметь возможность быть протестированным независимо.

6.5.7 Рабочий проект

На этапе рабочего проекта определяются:

– алгоритмы обработки и другие решения для программного обеспечения программных блоков (модулей), определенных на этапе технического проекта;

– процедуры тестирования, которые должны быть выполнены на этапе индивидуального тестирования программных модулей;

– предварительная редакция процедур тестирования при интеграции программных модулей.

6.5.8 Рабочее программирование

6.5.8.1 На этапе рабочего программирования (кодирования) алгоритмы, определенные в комплекте документации рабочего проекта, переводятся в инструкции, которые могут быть выполнены аппаратными средствами.

6.5.8.2 Кодирование выполняется в соответствии с принятыми в проекте стандартами на представление, структуру и комментарии в отношении исходных текстов программ.

6.5.8.3 После окончания кодирования программных модулей должно быть проведено их индивидуальное тестирование.

6.5.8.4 На этапе индивидуального тестирования каждый программный блок (модуль) подвергается независимому тестированию в соответствии с процедурами тестирования, разработанными на этапе рабочего проекта.

6.5.8.5 Целью тестирования является проверка того, что разработанные программные блоки отвечают спецификациям тестирования, разработанным на этапе рабочего проекта, выполняют предписанные им функции и не выполняют никакие другие действия.

6.5.8.6 После окончания индивидуального тестирования программных модулей должна проводиться их интеграция.

6.5.8.7 Этап интеграции состоит из последовательного объединения программных блоков в единое целое в соответствии с планом интеграции. При этом план интеграции должен содержать тесты, выполняемые на взаимосвязанных программных блоках и план выполнения такого тестирования.

6.5.8.8 В течение этапа интеграции должна выполняться специальная процедура регистрации обнаруженных несоответствий и их устранения. Результаты должны фиксироваться в форме, дающей возможность проверить их лицам, непосредственно не вовлеченным в процесс тестирования.

6.5.8.9 При разработке ПС на стадии проектирования и кодирования необходимо руководствоваться следующими требованиями:

– ПС системы должно обеспечивать непрерывный самоконтроль, контроль ТС системы, а так же контроль целостности внутрисистемных связей, что является основным фактором в выполнении требований по надежности всей системы в целом;

– структура прикладных программ должна быть модульной;

– структура прикладных программ должна быть простой и доступной для восприятия в отношении общей концепции и отдельных составляющих, при этом следует избегать применения различного рода «хитрых» приемов программирования, рекурсивных структур и сжатия кода;

– исходный текст программы в окончательной редакции должен быть легко просматриваемым от начала до конца;

– разработанное ПС должно быть обеспеченно качественной документацией.

6.5.8.10 На основе вышеизложенных принципов при проектировании и кодировании ПС должны быть учтены следующие общие рекомендации:

– на начальном этапе необходимо разработать меры, обеспечивающие требуемую надежность системы, включая систему автоматического контроля;

– метод разработки «сверху вниз» является более предпочтительным, чем метод «снизу вверх»;

– перед разработкой проекта по созданию ПС необходимо принять концептуальную модель структуры системы;

– любые прикладные программы должны быть разработаны таким образом, чтобы обеспечивалась простота их тестирования;

– при использовании стандартных ПС производителя или поставщика необходимо выполнить проверку правильности функционирования этого ПС.

6.5.8.11 Этап проектирования ПО должен завершаться выпуском официального документа «Спецификация характеристик ПО».

Данный документ служит основой официального анализа результатов этапа проектирования и служит основой для этапа кодирования. Документ должен быть достаточно подробным, чтобы рабочее программирование могло выполняться без дальнейших уточнений проекта.

6.5.8.12 Структура документа должна предусматривать возможность последующего расширения, выполняемого параллельно с процессом проектирования.

6.5.8.13 Состав и содержание «Спецификация характеристик ПО» должны разрабатываться в соответствии с нормативным документом 58413824.23512.001-390.РД-01-2002.М [5], с учетом требований NS-G-1.1 [6], представлены в собственных процедурах Разработчика и согласованы с Заказчиком.

6.5.9 Интеграция ТС системы и ее ПС

6.5.9.1 Процесс интеграции является процессом объединения в законченную систему прошедших проверки и испытания ТС системы и программных модулей, которая будет способна выполнить заданные проектные функции.

6.5.9.2 Интеграция включает в себя следующие этапы:

– сборку ТС в систему в соответствии с КД на систему путем их взаимного соединения;

– компоновку программных модулей в процессе установления их взаимосвязи;

– загрузку ПО в аппаратные модули;

– проверку путем тестирования на соответствие требованиям по взаимодействию аппаратных и программных средств, а также тестирование способности ПС функционировать при конкретной конфигурации системы.

6.5.10 План интеграции

6.5.10.1 План интеграции системы должен быть разработан в соответствии с рекомендациями ГОСТ Р МЭК 60880 и документально оформлен в соответствии с требованиями к процессу интеграции и проверен на соответствие требованиям к системам, важным для безопасности АС.

6.5.10.2 План интеграции системы должен содержать описание организационных и процедурных аспектов интеграции аппаратных и программных средств.

6.5.10.3 План интеграции системы необходимо подготовить на достаточно раннем этапе разработки, чтобы требования к процессу интеграции системы можно было включить в проект разработки аппаратных и программных средств.

6.5.10.4 В плане указываются стандарты и процедуры, по которым выполняется интеграция аппаратных и программных средств, и документально фиксируются положения общего плана проверки качества, в соответствии с которыми выполняется интеграция системы.

6.5.10.5 План интеграции системы должен содержать все ограничения, которые возникают в результате специфического проектирования ТС и программного обеспечения. В план должны быть включены требования к процедурам и методам контроля, включая:

– управление конфигурацией системы;

– интеграцию системы;

– тестирование интегрированной системы;

– устранение ошибок.

6.5.11 Управление конфигурацией системы

6.5.11.1 В плане интеграции системы должна быть определена библиотека программных и аппаратных модулей, предназначенная для управления конфигурацией системы. Такая библиотека должна обеспечивать управление всеми используемыми в системе аппаратными и программными модулями.

6.5.11.2 Должны быть разработаны процедуры использования библиотеки с учетом следующих требований:

– процедура должна позволять до выполнения проверки включать в библиотеку модуль или его отредактированные версии;

– процедура должна обеспечить интеграцию системы с использованием отредактированных версий отдельных модулей;

– процедура должна предусматривать создание указателя частоты использования любого модуля системы так, чтобы при последующей редакции модуля можно было правильно оценить его роль;

– процедура не должна вступать в противоречие с общим планом контроля качества.

6.5.11.3 Конкретные процедуры интеграции аппаратных и программных средств зависят от характера проектирования системы. Такие процедуры необходимо сформулировать и отразить в плане интеграции, включив в них следующие положения:

– сборка требуемых модулей с использованием библиотеки и разработанных процедур;

– интеграция аппаратных модулей в систему (например, размещение модулей, адрес памяти, выбор, соединения);

– установка связей между модулями ПС и загрузка ПС в аппаратный комплекс;

– предварительное функциональное тестирование интегрированной системы;

– документальное оформление процесса интеграции и выбор конфигурации системы для выполнения верификационного тестирования;

– формальный документ о допуске интегрированной системы к верификационным испытаниям.

6.5.11.4 Выполняемое на данном этапе тестирование является функциональным тестированием системы, которое выполняет Разработчик.

6.5.11.5 Любые обнаруженные при таком тестировании ошибки, являются ошибками самой интеграции и не влияют на какой-либо документ проекта, поэтому их можно устранить, не составляя формальный отчет об ошибках. Однако если устранение какой-либо из ошибок требует внесения изменения в уже прошедшее

проверку ПС или внесения изменений в проектную документацию, то по такой ошибке составляется отчет.

6.5.12 Применение ранее разработанного (апробированного) ПС

6.5.12.1 Если в проекте применяется ранее разработанное (апробированное) ПС, его правильная работа должны быть доказана. При этом во внимание принимается:

– оценка поставщика программного обеспечения;

– эксплуатационный опыт и архивные данные по работе программного обеспечения:

а) пользователей, которые применяли это программное обеспечение;

б) время, в течение которого это программное обеспечение активно использовалось;

– доказательство того, что существует документация на это программное обеспечение, а также отслеживание и исправление ошибок в нем.

6.5.12.2 К системам, имеющим класс безопасности, применяются требования нормативного документа 58413824.23512.001-390.РД-01-2002.М [5], с учетом требований NS-G-1.1 [6].

6.5.13 Требования к верификации ПС

6.5.13.1 После установления функциональных требований к ПС и до начала следующего этапа, верификация должна затрагивать вопросы соответствия функциональных требований, предъявляемых к ПС и определенных спецификацией требований к управляющей системе.

6.5.13.2 После этапа проектирования и до начала следующего этапа, верификация должна затрагивать вопросы соответствия ПС (согласно приведенным в спецификации характеристик ПС), функциональным требованиям к ПС.

6.5.13.3 После этапа кодирования и до начала следующего этапа, верификация должна затрагивать вопросы соответствия закодированного ПС спецификации характеристик ПС, разработанной на этапе разработки проекта.

6.5.13.4 В качестве дополнительного требования для программного обеспечения, имеющего класс безопасности, является независимость группы верификации от группы разработки.

6.5.13.5 Для программного обеспечения, имеющего второй класс безопасности, обязательным является верификация независимым лицом или организацией.

6.5.14 План верификации

6.5.14.1 План верификации должен определять все критерии, технологии и средства, используемые в процессе верификации и описывать работы, которые необходимо провести для оценки каждого элемента программного обеспечения и каждого этапа, чтобы показать, выполняются ли спецификации требований по функциональности и надежности.

6.5.14.2 Уровень детализации Плана верификации должен быть таким, чтобы независимая группа верификации могла выполнить программу верификации и выработать объективное мнение по вопросу - удовлетворяет ли ПС предъявляемым к нему требованиям по своим характеристикам или нет.

6.5.14.3 План верификации должен быть разработан в соответствии с требованиями и рекомендациями стандартов (IEEE Std 1012 [3], ГОСТ Р МЭК 60880).

6.5.14.4 План верификации ПС должен быть согласован с Заказчиком и содержать следующие разделы:

– цель верификации ПС;

– справочная и нормативная документация;

– определения;

– общие положения по проведению верификации ПС;

– организационная структура группы верификации ПС;

– комплексный график проведения верификации ПС;

– необходимые ресурсы при проведении верификации ПС;

– распределение обязанностей ответственных лиц и исполнителей при проведении верификации ПС;

– инструментальные средства, процедуры и методики, используемые при проведения верификации ПС;

– мероприятия по верификации на этапах жизненного цикла ПС, в том числе:

а) управление проведением верификации ПС;

б) мероприятия по верификации на этапе разработки требований к системе;

в) мероприятия по верификации на этапе разработки требований к ПС;

г) мероприятия по верификации на этапе проектирования ПС;

д) мероприятия по верификации на этапе кодирования;

е) мероприятия по верификации на этапе тестирования ПС;

ж) мероприятия по верификации на этапе инсталляции ПС на аппаратные средства и его отладки;

з) мероприятия по верификации на этапе комплексных испытания управляющей системы, важной для безопасности;

и) мероприятия по верификации на этапе ввода управляющей системы, важной для безопасности в эксплуатацию на объекте;

к) мероприятия по верификации на этапе эксплуатации и обслуживания ПС;

– отчетность по проведению мероприятия по верификации ПС;

– административные процедуры мероприятия по верификации, в том числе:

а) отчетность по несоответствиям и их устранению;

б) процедуры контроля выполнения плана верификации ПС;

в) отклонение от плана;

– используемые стандарты, методики и принятые соглашения.

6.5.15 Отчетные документы по верификации ПС

6.5.15.1 Отчетные документы по верификации должны дать исчерпывающие ответы на все вопросы, которые должны быть рассмотрены на всех этапах верификации ПС.

6.5.15.2 При формировании отчетных документов по верификации наиболее удобно пользоваться контрольными таблицами.

6.5.15.3 Контрольные таблицы каждого этапа верификации должны быть разработаны в соответствии с рекомендациями ANSI/ANS-10.4, представлены в собственных процедурах организации-разработчика, согласованы с Заказчиком.

6.6 Модификации

6.6.1 Любая модификация, что бы ни послужило ее первопричиной, должна приводить к формированию комплекта документации по модификации, содержащего в том числе:

– запрос на модификацию;

– оценку осуществимости модификации, состоящую из проверки последствий для аппаратных средств и программного обеспечения и оценку объема операций, необходимых для того, чтобы выполнить, проверить правильность работы и аттестовать модификацию.

6.6.2 Выполнение модификаций должно осуществляться в соответствии с планом обеспечения качества.

6.6.3 Все документы, которых коснулась модификация, должны быть исправлены и в них внесена ссылка на запрос на модификацию. В отчете по модификации должны быть описаны все предпринятые действия.

6.6.4 Эти документы датируются, нумеруются и составляются в комплект, чтобы оформить идентифицируемую версию программного обеспечения.

6.6.5 Для программного обеспечения УСВБ, применяются требования ГОСТ Р МЭК 60880.

7 Квалификация оборудования

7.1 Общие положения

7.1.1 Целью квалификации оборудования является подтверждение того, что оборудование, входящее в состав УСВБ может гарантировано выполнить все предусмотренные проектом функции с требуемым качеством в течение всего назначенного срока службы при наиболее неблагоприятных, тяжелых сочетаниях воздействий условий окружающей среды до, во время и после протекания проектных аварий.

7.1.2 Эти условия окружающей среды должны учитывать ожидаемые изменения в условиях нормальной эксплуатации, отклонения от нормы (ожидаемые

переходные процессы), аварийные условия, поставарийное состояние, а также условия испытаний герметических ограждений (для оборудования, устанавливаемого в герметических ограждениях).

7.1.3 Там, где оборудование может быть подвержено влиянию сейсмических воздействий, в рамках событий заложенных в проекте, и должно обеспечивать безопасность, как во время события, так и после него, программа квалификации должна включать эти возможные сейсмические воздействия, под влиянием которых может находиться оборудование.

7.1.4 Допускается применение нескольких методов квалификации. Факторами, влияющими на выбор используемого метода, обеспечивающего надлежащую квалификацию, являются:

– специфические функции оборудования, выполняемые им в случае проектной аварии, включая сейсмические воздействия;

– условия окружающей среды в помещениях, где это оборудование установлено;

– возможные проектные сейсмические воздействия.

7.1.5 Для проведения квалификации оборудования могут использоваться следующие методы:

– прямые испытания;

– опыт эксплуатации;

– анализ;

– комбинированный метод.

7.1.6 Применимость каждого метода должна быть обоснована. Кроме того, должны быть учтены требования национальных и международных стандартов, которые касаются испытаний на воздействие окружающей среды и которые могут быть применены к электрическому оборудованию УСВБ подпадающему под действие настоящих Общих положений.

7.1.7 Методы квалификации, установленные настоящими Общими положениями, должны использоваться как для первоначальной квалификации оборудования, так и при последующих квалификациях модернизированного оборудования.

7.2 Порядок проведения квалификации

7.2.1 Процедура квалификации должна начинаться с выполнения следующих мероприятий:

– разработки подробного перечня оборудования УСВБ которое должно быть квалифицировано;

– подготовки технических условий для каждого оборудования.

7.2.2 Оборудование должно быть классифицировано в зависимости от места его размещения и его роли в обеспечении безопасности.

7.2.3 Технические условия на оборудование УСВБ должно включать следующие характеристики и сведения:

– все нормальные и аварийные внешние условия, при которых оборудование используется;

– функции безопасности, которые должны быть выполнены;

– технические характеристики оборудования:

а) при нормальных условиях эксплуатации;

б) при отклонениях от условий нормальной эксплуатации;

в) при исходных событиях;

г) в условиях, установившихся после исходных событий;

– диапазоны напряжений, частоты, нагрузки, электромагнитных помех и другие электрические характеристики;

– основные характеристики всех электрических соединений;

– требования к установке, включая место размещения, метод монтажа и конфигурацию оборудования системы (в том числе необходимо указать, может ли быть оборудование подвержено воздействию аварийных условий);

– объем и периодичность профилактического обслуживания для обеспечения установленного срока службы оборудования;

– проектный срок службы оборудования и проектный срок службы его компонентов, которые имеют меньший срок службы, чем оборудование в целом;

– органы управления, показывающие и другие вспомогательные приборы, включенные в состав оборудования, а также внешние приборы, необходимые для правильной работы оборудования;

– диапазон, характерные периодичность и длительность воздействий окружающей среды, включая температуру, давление, влажность, уровень радиации, химическое и сейсмическое воздействие;

– полное описание рабочего цикла оборудования и число рабочих циклов, включая периодические испытания;

– срок квалификации оборудования (характеристика должна соответствовать техническим условиям или техническому заданию на оборудование).

7.3 Квалификация оборудования прямым испытанием

7.3.1 Общие требования

7.3.1.1 Прямое испытание образца оборудования имитацией условий эксплуатации является наиболее предпочтительным методом. Этот метод должен использоваться для большей части аппаратуры при первоначальной квалификации.

7.3.1.2 Прямое испытание предназначено для того, чтобы продемонстрировать соответствие (или превышение) характеристик оборудования тем требованиям, которые приведены в технических условиях или техническом задании на это оборудование.

7.3.1.3 Прямое испытания должно состоять из планомерной последовательности испытательных условий, которые соответствуют (или превышают их) проектным условиям эксплуатации, включая квалификационный запас, и должны учитывать возможность эксплуатации оборудования в нормальных, переходных и аварийных условиях.

7.3.1.4 Критерии проведения данных испытаний должны устанавливаться с учетом рабочих характеристик оборудования, условий энергообеспечения и внешних проектных условий, а так же пределов рабочих характеристик оборудования, связанного с безопасностью, как при изменении условий подачи

электропитания и его характеристик, так и при изменении условий окружающей среды.

7.3.1.5 Во время проведения серии испытаний должно использоваться одно и то же оборудование. В соответствии с национальными и международными стандартами последовательность испытания должна быть наиболее жесткой. Тем не менее, серия испытаний будет считаться проведенной в наиболее жестких условиях, в случае, если в условиях данного испытания его результаты окажутся представительными, по отношению к фактическим режимам эксплуатации конкретного оборудования.

7.3.2 Программа испытаний

7.3.2.1 Программа испытаний должна соответствовать техническим условиям на оборудование, подробно описывать необходимые испытания и обеспечивать «связь» между техническими условиями и результатами испытаний.

7.3.2.2 Программа испытаний должна содержать:

– описание оборудования;

– данные о количестве испытываемых образцов;

– требования к монтажу, а также механическим и электрическим соединениям;

– описание процедуры ускоренного старения;

– условия эксплуатации и окружающей среды, которые должны быть смоделированы;

– критерии, по которым проверяются характеристики оборудования, включая параметры, которые должны быть измерены;

– требования к испытательному оборудованию, включая точность;

– допустимые пределы измерения характеристик оборудования;

– перечень требований, по которым испытания не проводятся;

– описание других возможных условий, не упомянутых выше, которые могут быть специфичными для оборудования и могут повлиять на его работу во время испытаний.

7.3.3 Контроль параметров при испытаниях

7.3.3.1 Контроль параметров в ходе испытаний должен осуществляться приборами, достаточно точными для обнаружения сколько-нибудь значимых изменений в величинах переменных.

7.3.3.2 Испытательное оборудование должно быть откалибровано в соответствии с установленными стандартами, что должно быть подтверждено документально.

7.3.3.3 Интервал между измерениями должен быть таким, чтобы получить зависимость каждого измеряемого параметра от времени.

7.3.3.4 При описании процедур испытания факторы воздействия могут быть разделены на следующие категории:

– окружающие условия (температура, давление, влажность, состав газов, вибрация, время и т.д.);

– входные электротехнические характеристики оборудования (частота, ток, напряжение, мощность электропитания, подводимого к квалифицируемому оборудованию);

– характеристика жидкостей (концентрация химических веществ в жидкостях, впрыскиваемых в испытательную камеру, расход жидкостей, расположение впрыска и температура жидкостей);

– характеристики радиоактивного излучения (данные по радиоактивному излучению, включающие тип, энергетический уровень, интенсивность и дозу облучения);

– электротехнические характеристики оборудования (сопротивление изоляции электрических компонентов, выходное напряжение, выходной ток и мощность; время срабатывания, частотные характеристики и имитируемая нагрузка);

– механические характеристики (растяжение, крутящий момент, график изменения нагрузки во времени и т.д.)

7.3.3.5 Могут применяться некоторые другие характеристики, такие как:

– наведенные и излучаемые электромагнитные помехи;

– переходные электрические процессы системы электрического питания.

7.3.4 Квалификационный запас

7.3.4.1 Квалификационные прямые испытания должны включать проверку существования необходимого квалификационного запаса. Повышение испытательных уровней, увеличение количества испытательных циклов и продолжительности испытаний должны рассматриваться как метод обеспечения необходимого квалификационного запаса.

7.3.4.2 При отсутствии подробных технических требований при проведении прямых испытаний предлагаются следующие значения квалификационного запаса, при которых оборудование должно продолжать выполнять свои функции:

– напряжение питания от плюс 10% до минус 15% от номинального значения, если не указано другое;

– частота ±5% от номинального значения, если не указана другая

– термодинамические параметры в аварийных условиях:

а) температура насыщенного пара: запас должен быть выбран таким образом, чтобы возникающее во время испытаний давление не превышало давление насыщенного пара при максимальной рабочей температуре более чем на 1×10^5 Па;

б) давление: плюс 10% относительно давления насыщенного пара, но не больше, чем 1×10^5 Па;

в) время: плюс 10% относительно периода времени, в течение которого оборудование должно быть работоспособным после возникновения проектной аварии;

г) переходные процессы: должны быть проведены испытания либо для одного переходного процесса (давление/температура) с квалификационным запасом, либо для двух переходных процессов без квалификационного запаса.

– интегральные величины старения и аварийной дозы излучения: плюс 10 % от теоретически рассчитанной величины.

7.3.5 Последовательность проведения прямого испытания

7.3.5.1 Прямые испытания оборудования должны проводиться в определенной последовательности.

7.3.5.2 Выделяют три группы испытаний:

– группа 1 включает:

а) проверку функциональных характеристик при нормальных условиях, а также при всех специально установленных режимах эксплуатации;

б) внешний осмотр. Внешний осмотр оборудования проводится для того, чтобы убедиться, что испытываемая единица не была повреждена после ее изготовления в результате неправильного обращения, а также, чтобы проверить ее соответствие техническим условиям;

в) проверку характеристик оборудования при нормальных условиях окружающей среды. Проверка проводится, чтобы получить данные для сравнения с характеристиками его работы при более тяжелых условиях. На этом этапе могут выполняться определенные измерения, например для построения графиков изменения параметров во времени. В это время должны быть определены соответствующие параметры, такие как величина погрешности или ухода показания.

Основная методология измерения таких параметров должна соответствовать рекомендациям ГОСТ Р МЭК 61298-2;

г) Испытания оборудования при предельных значениях эксплуатационных и электротехнических параметров. Во время проведения этих испытаний оборудование должно работать при предельных значениях эксплуатационных и электротехнических параметров, указанных в его технических условиях, в том числе:

1) при указанных пределах рабочего напряжения (или частоты) питания;

2) при предельных значениях температурного диапазона;

3) при наличии электрических или электромагнитных помех, наведенных и (или) излучаемых (в соответствии с рекомендациями ГОСТ Р 51317.4.1).

Во время испытаний при предельных условиях эксплуатации необходимо проверять, остаются ли значения характеристик, измеренных во время фазы в), в пределах, указанных в технических условиях на данное оборудование.

– группа 2 включает проверку сейсмостойкости оборудования.

Если старение является существенным фактором для данного оборудования, то перед испытаниями на сейсмостойкость оборудование должно быть предварительно состарено;

– группа 3 включает проверку стойкости оборудования к аварийным и поставарийным условиям:

а) оценка изменения характеристик оборудования с течением времени.

Оборудование должно быть подвергнуто процессу старения, чтобы привести его в состояние, имитирующее условия, характерные для предполагаемого полного срока службы, при этом должны быть учтены следующие факторы, влияющие на процесс старения:

1) температура (циклически меняющаяся и постоянная);

2) коррозия;

3) воздействие борных и дезактивирующих растворов;

4) длительная работа;

5) облучение, соответствующее дозе, которая будет накоплена оборудованием за весь срок службы;

6) механическая вибрация;

б) испытания при аварийных и поставарийных условиях.

Эти испытания предназначены для проверки работы оборудования, поставленного в аварийные условия, такие как:

1) землетрясение (или другие явления, связанные с вибрацией, такие как падение самолета и ударная волна);

2) облучение с накопленной дозой, соответствующей дозе, которой подвергается оборудование в результате возникновения исходных событий (термодинамическая авария внутри герметических ограждений);

3) внезапное воздействие насыщенного пара (резкое возрастание давления и температуры), имитирующее аварию внутри герметических ограждений;

4) воздействие насыщенного пара в течение послеаварийной фазы, следующей за внутренней термодинамической аварией внутри герметических ограждений.

7.3.5.3 Группа 1 относится к общепромышленным испытаниям.

7.3.5.4 Испытания, приведенные в группах 2 и 3 рассчитаны, в основном, для оборудования, применяемого на АС и имеют свои особенности.

7.3.5.5 Испытания по трем группам могут производиться независимо и на различных образцах оборудования.

7.3.5.6 При проведении испытаний, относящихся к группе 1, следует применять стандартизованные методики для общепромышленной группы оборудования.

7.3.5.7 При проведении испытаний, относящихся к группам 2 и 3 следует разрабатывать методики испытаний с учетом требований национальных стандартов, методических рекомендаций Генпроектировщика АС, проводившего соответствующие изыскания при выборе площадки для строительства АС, международных нормативных документов. Рекомендации по применению процедур испытаний приведены в IEC/IEEE 60780-323 [1].

7.4 Квалификация оборудования опытом эксплуатации

7.4.1 Общие требования

7.4.1.1 Квалификация оборудования УСВБ, проводимая на основе опыта эксплуатации, должна включать:

– временную зависимость характеристик и условий эксплуатации квалифицируемого типа оборудования;

– взаимосвязь между существующими и проектными условиями эксплуатации;

– доказательство того, что рабочие параметры оборудования соответствуют или даже превышают требования к нему при проектных условиях эксплуатации.

7.4.1.2 Комбинированная квалификация на основе опыта эксплуатации, типовых испытаний и анализа также может использоваться, особенно для оборудования, размещаемого внутри здания реактора.

7.4.2 История эксплуатации

7.4.2.1 Для проведения квалификации с помощью опыта эксплуатации должна быть представлена документация о внешних условиях для квалифицируемого оборудования и устройств его сопряжения.

7.4.2.2 Эта документация должна содержать данные о физическом размещении и монтаже оборудования на работающей установке.

7.4.2.3 Характеристики квалифицируемого электрического оборудования данного типа и его устройств сопряжения должны определяться либо исходя из данных измерений, либо на основе анализа реальных отказов, либо с помощью обоих этих методов.

7.4.2.4 Документация, касающаяся характеристик систем, важных для безопасности, должна содержать:

– рабочие характеристики оборудования, полученные по результатам измерений или из технических условий на оборудование;

– данные по всем отказам с анализом этих отказов и тенденций, наблюдавшихся в течение периода эксплуатации;

– записи о периодическом обслуживании и проверках (включая настройку и калибровку).

7.4.3 Процесс квалификации

7.4.3.1 С помощью документации необходимо показать, что оборудование, чья история эксплуатации взята при квалификации оборудования за основу, является типовым для любого оборудования, имеющего то же обозначение.

7.4.3.2 Можно считать, что оборудование прошло квалификационные испытания, если будет показано, что:

– зарегистрированные условия эксплуатации данного типа оборудования по жесткости соответствуют или превосходят проектные условия эксплуатации;

– характеристики эксплуатируемого оборудования соответствуют или превосходят требования, предъявляемые пользователем.

7.4.3.3 Должно быть отмечено, что если проектом предусмотрены сейсмические воздействия с последующим воздействием исходного события более жестким, чем те, что были зафиксированы в процессе эксплуатации, то установленное оборудование должно быть подвергнуто частичным типовым испытаниям.

7.4.3.4 При этих испытаниях оборудование должно быть подвергнуто сейсмическому воздействию, а также воздействию исходных событий проектной аварии, после чего оборудование может считаться полностью прошедшим квалификацию.

7.5 Квалификация оборудования на основе анализа

7.5.1 Общие требования

7.5.1.1 При квалификации на основании анализа необходимо доказать, что если оборудование подвергнется воздействию внешних условий, установленных для нормальной эксплуатации, или воздействию исходных событий, установленных для проектной аварии, то его, связанные с безопасностью, характеристики будут удовлетворять установленным требованиям.

7.5.1.2 В общем случае это доказательство должно быть основано на общепринятых принципах, данных опыта эксплуатации, данных частичных типовых испытаний или комбинацией вышеупомянутых данных. Все допущения, включая экстраполяцию, должны быть, обоснованы с указанием использованных принципов и проверяемых данных испытаний. Анализ должен быть представлен в форме, которая может быть легко понята и проверена.

7.5.2 Методы квалификации на основе анализа

7.5.2.1 При проведении анализа могут использоваться следующие аналитические методы:

– определение подобия;

– экстраполяция;

– математическое моделирование.

7.5.2.2 Метод определения подобия может использоваться для оценки данного изделия посредством демонстрации его сходства с уже квалифицированным изделием. Данный метод главным образом используется при проведении типовых испытаний для квалификации идентичного оборудования.

7.5.2.3 Экстраполяция является одним из методов анализа, который может быть использован в дополнение к испытаниям. Обоснование этого метода проводится на

индивидуальной основе. Однако этот метод квалификации оборудования УСВБ допускается использовать только в том случае, когда виды отказов, наблюдаемые при интенсификации или ускорении воздействий внешней среды и прогнозируемые виды отказов при требуемых условиях эксплуатации одинаковы.

7.5.2.4 Метод математического моделирования предполагает разработку верифицированной математической модели квалифицируемого оборудования. При этом математическая модель должна основываться на установленных закономерностях, представительных результатах испытаний или эксплуатационного опыта для демонстрации того, что при реальных рабочих условиях оборудование может выполнять свои функции.

7.5.3 Процесс квалификации

7.5.3.1 Типовое электрическое оборудование считается прошедшим квалификацию, если показано, что в течение всего срока квалификации значения характеристик оборудования соответствуют или превосходят требования технических условий для наиболее жестких внешних воздействий или последовательности внешних воздействий.

7.5.3.2 Степень жесткости параметров внешней среды должна быть основана на знании вида и механизмов отказов оборудования, выявляемых в процессе испытаний.

7.5.3.3 Если для построения математической модели использовалось испытание на ускоренное старение, то срок квалификации должен базироваться на знании пределов экстраполяции зависимых от времени результатов воздействия окружающей среды.

7.6 Комбинированная квалификация

7.6.1 Оборудование может быть квалифицировано с помощью типовых испытаний, опыта предыдущей эксплуатации, анализа или какой-либо комбинацией этих трех методов. Если габаритные размеры, условия применения, время или другие ограничения препятствуют проведению полномасштабных типовых

испытаний, могут быть проведены частичные типовые испытания оборудования, дополненные испытаниями отдельных его компонентов.

7.6.2 Частичные типовые испытания с анализом, опыт эксплуатации с анализом и дополнительные типовые испытания отдельных компонентов с анализом являются примерами проведения комбинированной квалификации.

7.7 Квалификация работающего оборудования

7.7.1 На действующих энергоблоках квалификация работающего оборудования обычно проводится только для оборудования выполняющего функции безопасности во время и/или после исходного события.

7.7.2 При проведении квалификации этого оборудования может оказаться, что срок его службы меньше, чем предполагаемый срок службы энергоблока. В этом случае могут быть применены следующие процедуры:

– замена всего оборудования или его ответственных частей в течение заранее определенного периода времени;

– периодическая проверка соответствующих параметров работающего оборудования (точности, сопротивления изоляции, времени отклика и т.п.).

7.7.3 Замененное оборудование должно быть установлено и эксплуатироваться на АС при внешних воздействующих факторах соответствующих техническим условиям на это оборудование и не ускорять процесс его старения.

7.7.4 Если условия эксплуатации оборудования более жесткие, чем это определено в технических условиях на него (что может ускорить процесс его старения), то это оборудование должно быть демонтировано после заранее определенного периода времени, который меньше срока его квалификации или срока квалификации оборудования этого же типа. Затем это оборудование должно быть подвергнуто квалификационным испытаниям, аналогичным тем, которые были проведены до его установки, включая испытание на ускоренное старение.

7.7.5 Успешное завершение этих испытаний означает продление срока квалификации оборудования.

7.7.6 Эта процедура должна повторяться до тех пор, пока срок квалификации оборудования не станет равным требуемому сроку энергоблока.

7.7.7 При соответствующем обосновании могут быть применены и другие эквивалентные методы.

7.8 Критерии отказа

7.8.1 При оценке результатов квалификационных испытаний любой образец оборудования считается отказавшим, если оборудование не выполняет функции, которые указаны в технических условиях на него.

7.8.2 Особо должен быть рассмотрен случай, когда оборудование прошло такие испытания, но показало явное ухудшение своих параметров.

7.9 Отчет о проведении квалификации оборудования

Отчет о проведении квалификации оборудования должен включать в том числе:

– идентификацию квалифицируемого оборудования (например, ссылку на комплект документации по идентификации оборудования);

– ссылки на документы, детализирующие метод квалификации;

– названия организации (организаций), проводящих квалификацию оборудования;

– отчеты, по всем этапам квалификации, включая полученные результаты;

– упоминание о любых инцидентах, произошедших при проведении квалификации (неудовлетворительные результаты, отказы оборудования и т.д.), с детальным перечислением предпринятых последующих действий (описание ремонтов, характер модификаций/модернизаций, выполненных на модели, условия, регулирующие повторение испытаний, проведение дополнительных испытаний и т.д.);

– результирующие выводы о том, что оборудование соответствует спецификации на испытания, или перечень выявленных несоответствий.

7.10 Определение категории квалификации оборудования

7.10.1 Основные принципы категоризации

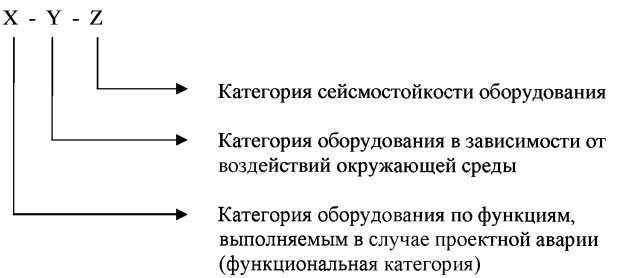
7.10.1.1 Оборудование УСВБ должно быть квалифицировано:

– в соответствии с его специфическими функциями, выполняемыми им в случае проектной аварии, включая сейсмические события;

– по условиям окружающей среды в помещениях, где это оборудование установлено;

– в зависимости от возможных проектных сейсмических воздействий.

7.10.1.2 Идентификация оборудования по категориям осуществляется по следующей схеме:



7.10.2 Функциональные категории

7.10.2.1 К первой функциональной категории относится оборудование, которое в пределах проектных авариях должно функционировать и способствовать ликвидации последствий таких аварий. Это оборудование должно быть квалифицировано, чтобы доказать его работоспособность в условиях аварии в течение времени, требуемого для ликвидации последствий аварии, с определенным допуском (запасом) до отказа этого оборудования.

7.10.2.2 Ко второй функциональной категории относится оборудование, которое при проектных авариях и их ликвидации не должно функционировать. Отказ этого оборудования не должен негативно влиять на ликвидацию аварии или безопасность станции. Это оборудование должно быть квалифицировано, чтобы продемонстрировать способность сохранить целостность своих качеств в любых

аварийных условиях с определенным допуском (запасом) и/или не влиять на ликвидацию аварии.

7.10.2.3 К третьей функциональной категории относится оборудование, которое не выполняет функций по ликвидации последствий аварий и отказ которого (во всех режимах) не может отрицательно повлиять на безопасность АС или помешать действиям по ликвидации последствий аварии. Это оборудование не требует квалификации для каких-либо аварийных условий.

7.10.2.4 Оборудование, важное для безопасности, которое не квалифицируется для каких-либо проектных аварий, тем не менее, должно квалифицироваться чтобы доказать свою работоспособность в ожидаемых предельных условиях эксплуатации при неаварийной обстановке.

7.10.3 Категория окружающей среды

При квалификации оборудования рассматриваются следующие категории окружающей среды:

Н - категория окружающей среды в помещениях, в которых размещаемое оборудование должно быть квалифицировано для подтверждения функционирования и/или подтверждения электрических, механических характеристик и/или характеристик отказоустойчивости (отсутствие отказов) в «тяжелых условиях»;

М - категория окружающей среды в помещениях, в которых размещаемое оборудование должно быть квалифицировано для подтверждения функционирования и/или подтверждения электрических, механических характеристик и/или характеристик отказоустойчивости (отсутствие отказов) в «щадящих» условиях.

7.10.4 Категория сейсмостойкости

7.10.4.1 Оборудование УСВБ квалифицируется по категории I сейсмостойкости для подтверждения как работоспособности (выполнение активных функций) так и структурной целостности (выполнение пассивных функций), при воздействии МРЗ.

К категории I сейсмостойкости относятся:

– системы безопасности, обеспечивающие поддержание активной зоны реактора в подкритичном состоянии, аварийный отвод тепла от реактора, локализацию радиоактивных продуктов;

– системы нормальной эксплуатации, важные для безопасности и их элементы, выход из строя которых, при сейсмических воздействиях до МРЗ включительно может привести к выходу радиоактивных продуктов в количествах, приводящих к дозовым нагрузкам на население сверх установленных значений для максимальной проектной аварии согласно действующим «Санитарным правилам проектирования и эксплуатации атомных станций» (СП АС-03);

– здания, сооружения, оборудование и их элементы, механическое повреждение которых при сейсмических воздействиях до МРЗ включительно путем силового воздействия на вышеупомянутые системы может привести к их отказу в работе.

7.10.4.2 Оборудование УСВБ квалифицируется по категории II сейсмостойкости для подтверждения как работоспособности (выполнение активных функций) так и структурной целостности (выполнение пассивных функций), при воздействии проектного землетрясения.

К категории II сейсмостойкости относятся здания, сооружения, конструкции, оборудование и их элементы (не вошедшие в первую категорию), нарушение работы которых в отдельности или совокупности с другими признаками может привести к недовыработке электроэнергии и/или к дозовым нагрузкам населения сверх допустимых годовых значений, установленным для нормальной эксплуатации действующими нормативными документами.

7.10.4.3 Оборудование, не связанное с безопасностью, должно быть проанализировано для подтверждения того, что его отказ в заданных условиях проектных аварий не приведет к отказу соответствующих функций безопасности систем безопасности и оборудования. В противном случае потребуется квалификация этого оборудования, соответственно, на сейсмостойкость и воздействие окружающей среды.

7.10.5 Примеры идентификации оборудования

7.10.5.1 Категория квалификации активного и пассивного оборудования УСВБ расположенного в «жестких» условиях окружающей среды:

– квалификационная категория 1 - Н - I в случаях, когда во время проектной аварии требуются активные функции оборудования;

– квалификационная категория 2 - Н - I (II) в случаях, когда во время проектной аварии активная функция оборудования не требуется.

7.10.5.2 Квалификация активного и пассивного оборудования УСВБ, расположенного в «щадящих» условиях окружающей среды:

– квалификационная категория 1 - М - I в случаях, когда во время проектной аварии требуются активные функции оборудования;

– квалификационная категория 2 - М - I (II) в случаях, когда во время проектной аварии активная функция оборудования не требуется.

7.10.5.3 Для оборудования УСВБ, относящихся к различным квалификационным категориям, применяется своя процедура квалификации, а именно:

– процедура квалификации П1 – для оборудования квалификационной категории 1 – Н – I;

– процедура квалификации П2 – для оборудования квалификационной категории 1 – Н – I(II);

– процедура квалификации П3 – для оборудования квалификационной категории 1 – М – I(II);

– стандартная (общепромышленная) процедура квалификации – для оборудования квалификационной категории 2 – М – I(II).

7.10.5.4 Все оборудование, входящее в состав УСВБ подвергается квалификации в соответствии с процедурами П1, П2, П3.

7.10.6 Процедуры квалификации

7.10.6.1 Детальные требования, которым должны удовлетворять процедуры квалификации оборудования перечисленных квалификационных категорий должны быть представлены в нормативном документе «Атомные станции. Управляющие

системы, важные для безопасности. Требования к процедурам квалификации оборудования различных квалификационных категорий».

7.10.6.2 Указанный нормативный документ должен быть разработан в развитие настоящих Общих технических требований.

8 Разработка пунктов управления

8.1 Общие требования к пунктам управления

8.1.1 Блочный пункт управления

8.1.1.1 Блочный пункт управления должен являться основным местом для операторов выполняющих действия, относящиеся к безопасности управления энергоблоком. БПУ должен обеспечивать безопасную эксплуатацию ЭБ во всех проектных режимах, и из которого могут быть приняты меры, чтобы поддерживать ЭБ в безопасном состоянии или вернуть его в такое состояние после начала ожидаемых при эксплуатации событий, проектных и запроектных авариях. Кроме того, с БПУ должны быть приняты меры управления для смягчения последствия тяжелых аварий.

8.1.1.2 Расположение автоматизированных рабочих мест АРМ, а также реализация человеко-машинного интерфейса ЧМИ с точки зрения возможностей предоставления информации для обеспечения контроля и управления технологическими процессами в различных состояниях (режимах) ЭБ должны обеспечивать операторам, иметь возможность представлять полную картину состояния и режимов работы ЭБ.

8.1.1.3 В методологию разработки БПУ должны быть заложены следующие принципы:

– определение основных функциональных компонент ЧМИ;

– разработка общей компоновки БПУ;

– определение и разработка требований к отдельным функциональным компонентам ЧМИ;

– разработка эскизного проекта БПУ с учетом требований к ЧМИ;

– разработка и создание масштабного макета БПУ для оценки принятых решений;

– разработка общих моделей поведения операторов на БПУ в различных ситуациях;

– проведения функционального анализа с учетом ЧМИ;

– разработка программы верификации и валидации проекта БПУ;

– определение требований, необходимых для подготовки операторов с использованием программно-технических средств.

8.1.1.4 В связи с тем, что в определенных проектом эксплуатационных режимах операторам придется одновременно выполнять действия по контролю и управлению различным оборудованием входящему в состав систем нормальной эксплуатации и систем безопасности используя для управления АРМ и элементы традиционного способа контроля и управления, то это необходимо учитывать при проведении функционального анализа, разработки моделей поведения операторов и расположения/распределения АРМ и технических средств в виде панелей/пультов на БПУ и на дополнительных пунктах управления.

8.1.1.5 При разработке БПУ и дополнительных пунктов управления необходимо особое внимание уделять эргономическому обеспечению (освещение, кондиционирование, температурный режим, шумоизоляция, общее цветовое решение и т.д.) которые могут оказывать негативное влияние на операторов при выполнении ими своих обязанностей.

8.1.1.6 При разработке БПУ и дополнительных пунктов управления должны быть учтены и решены ряд эргономических вопросов связанных с физическими ограничениями и пределами возможностей человека, как оператора:

– антропометрические характеристики;

– способности зрительного и слухового восприятия;

– способности воспринимать, обрабатывать и реализовывать полученную информацию, в том числе и в стрессовом состоянии;

– способности к адаптации при переходе от одного типа управления к другому.

8.1.1.7 Основные информационные функции БПУ состоят в том, чтобы обеспечить операторов достаточной и своевременной информацией касающейся состояния оборудования/систем ЭБ для всех эксплуатационных режимов и аварийных условий, установленных в проекте, и оптимизировать действия операторов как команды по контролю и управлению ЭБ.

8.1.1.8 В связи с тем, что БПУ является центром, в котором располагаются средства и элементы контроля и управления системами безопасности, систем связанных с безопасностью и систем, не влияющих на безопасность, необходимо их физически и функционально разделять, так же учитывать и эргономические требования к ним.

8.1.1.9 При разработке БПУ необходимо принимать во внимание различные аспекты человеческих и технических факторов могущих оказывать негативное влияние на операторов:

– различные типы рабочей нагрузки;

– возможности человеческой ошибки;

– время реакции оператора на внешние раздражители, такие как звуковая и световая сигнализация;

– контроль и управление различным оборудованием с использованием различных способов контроля и управления.

8.1.1.10 Должны быть предусмотрены необходимые и достаточные условия в рабочей окружающей среде БПУ, включая условия освещения, температуры и влажности, а также возможности направленные на уменьшение опасных условий/воздействий типа недопустимых уровней облучения, дыма и т.д. в среде/атмосфере БПУ.

8.1.1.11 В связи с тем, что функция обеспечения безопасности включает в себя отображение, сигнализацию, средства контроля и управления, обычно используемые во всех эксплуатационных режимах ЭБ, при разработке БПУ следует применять сбалансированное распределение средств во всех указанных условиях.

8.1.1.12 Действия автоматики для средств управления, связанных с безопасностью, следует использовать во всех случаях для того, чтобы не переносить их на оператора при выполнении функций безопасности.

8.1.1.13 Человеческий фактор должен учитываться при конкретизации всей совокупности целей направленных на обеспечение безопасности при контроле и управлении технологическими процессами в различных состояниях ЭБ, наиболее важными из которых следующие:

– представление информации средствами отображения на АРМ и традиционными средствами на ТС следует объединять в гармоничную совокупность, чтобы оптимизировать понимание операторами на БПУ состояния оборудования/систем и ЭБ в целом, а также для оптимизации действий операторов, необходимых для управления оборудованием/системами и ЭБ в целом;

– когда в процессе управления используются средства для отображения на АРМ, как средства подтверждающие информацию представленную на ТС, то основные источники информации следует по возможности располагать и конфигурировать так, чтобы операторы могли использовать оба источника информации с минимальными усилиями необходимыми для использования при анализе ситуации;

– отображение любой информации на БПУ необходимо предоставлять таким образом, чтобы любой оператор БПУ имел возможность контроля, проведения ее анализа и определения статуса оборудования/системы и ЭБ в целом;

– элементы/устройства управления и функционально связанное с ними отображение информации необходимо, насколько это, возможно, располагать так, чтобы облегчить действия оператора, особенно в стрессовых ситуациях;

– необходимо предоставлять операторам БПУ информацию о состоянии/статусе оборудования/систем ЭБ, таким образом, чтобы операторы могли однозначно определять последовательность поступления информации особенно в переходных и аварийных режимах;

– для отображения информации на БПУ могут использоваться параметры, поступающие от систем имеющих разные классы безопасности, в таких случаях информацию необходимо предоставлять дифференцированно с учетом ее важности;

– необходимо предоставлять операторам БПУ информацию о состоянии/статусе каналов СБ как на мониторах, так и на обобщенной мнемосхеме;

– данные (параметры, события, состояния, действия автоматики, диагностические сообщения о состоянии оборудования/систем и справочная информация) должны предоставляться в форме, удобной для ее восприятия и понятной для проведения анализа операторами.

8.1.1.14 При разработке БПУ необходимо принимать во внимание, что в случае возникновения неисправностей/отказов в оборудовании располагаемого на БПУ вызванные одним исходным событием, они не препятствовали выполнению требуемых функций безопасности другим оборудованием.

8.1.1.15 Так как БПУ является центром управления ЭБ во всех эксплуатационных режимах, в том числе и в аварийных, поэтому необходимо предусматривать ограничение доступа на БПУ.

8.1.1.16 Необходимо предусматривать процедуры обслуживания на БПУ, систем кондиционирования, освещения, связи и борьбы с пожаром, чтобы обеспечить операторам непрерывность проведения контроля и управления в случае возникновения отказа вышеуказанных средств.

8.1.2 Дополнительные пункты управления

8.1.2.1 Кроме БПУ, для управления ЭБ должны использоваться дополнительные пункты управления. Расположение и назначение дополнительных пунктов управления определяется при разработке ЭБ.

Дополнительные пункты управления должны включать:

– резервный пункт управления;

– местные пункты управления.

8.1.2.2 С РПУ должны выполняться следующие функции:

– управление системами безопасности;

– перевод реакторной установки в подкритическое состояние;

– поддержание РУ в подкритическом состоянии необходимое время;

– отвод тепла от РУ;

– контроль состояния РУ.

Выполнение указанных функций должно производится с использованием ТС связанных с системами безопасности. Для обеспечения возможности контроля и управления технологическими процессами СНЭ на РПУ могут устанавливаться программно-технические средства аналогичные БПУ.

8.1.2.3 РПУ должен быть обеспечен:

– средствами представления информации;

– элементами контроля и управления;

– различными видами связи;

– необходимой документацией;

– системами жизнеобеспечения.

8.1.2.4 РПУ должен быть отдельно расположен, физически и электрически разделен от БПУ, так, чтобы РУ могла быть переведена в безопасное состояние и находится в нем необходимое время, и могли быть определены наиболее важные параметры, характеризующие состояние систем безопасности и ЭБ в целом, в случае потери возможности определения этих параметров на БПУ.

8.1.2.5 Необходимо предусматривать перевод приоритета управления на РПУ и разделению оборудования БПУ и РПУ, когда с БПУ не производятся процедуры по контролю и управлению за состоянием ЭБ.

8.1.2.6 РПУ и средства для контроля и управления необходимо размещать и располагать соответствующим образом, чтобы персонал мог выполнять свои функциональные обязанности в полном объеме.

8.1.2.7 При разработке БПУ должны быть определены условия, при возникновении которых теряется возможность выполнения операторами функций контроля и управления с БПУ и необходим переход на РПУ.

8.1.2.8 При разработке РПУ необходимо обеспечить безопасные пути доступа операторов на РПУ, чтобы позволить операторам, покидающим БПУ, передвигаться с минимальными потерями времени к РПУ.

8.1.2.9 При разработке РПУ необходимо предусматривать условия и мероприятия для предотвращения несанкционированного доступа на РПУ.

8.1.2.10 При выполнении операторами функций контроля и управления с РПУ, средства контроля и управления технологическими процессами должны быть аналогичными тем, которые используются на БПУ.

8.1.2.11 Разработку БПУ и РПУ следует выполнять таким образом, чтобы любое исходное событие не могло одновременно приводить к отказу выполнения функций БПУ и РПУ.

8.1.2.12 МПУ – это специально организованные места для контроля и управления за определенными проектом вспомогательными системами и отдельным оборудованием ЭБ, а также отдельные щиты, стойки и т.д.

8.1.2.13 С МПУ должны осуществляться контрольные и управляющие функции за пределами БПУ/РПУ. К функциям МПУ должны быть отнесены:

– контроль и управление вспомогательным оборудованием/системой по месту расположения или вблизи от оборудования/системы;

– обеспечение безопасной работы вспомогательного оборудования путем его отключения/останова;

– обеспечение вспомогательного контроля за состоянием основного технологического оборудования ЭБ;

– обеспечение ведения и поддержания в эксплуатационных пределах вспомогательных технологических процессов.

8.1.2.14 МПУ являются средствами контроля и управления вспомогательными технологическими системами с помощью дополнительных операторов.

8.2 Общие требования к человеко-машинному интерфейсу

8.2.1 Контроль и управление технологическими процессами в различных эксплуатационных состояниях ЭБ должны включать:

– представление необходимой информации и параметров посредством автоматического измерения;

– представление необходимой информации и параметров посредством расчетных задач с использованием программно-технических средств;

– функции контроля и управления с использованием человеко-машинного интерфейса (ЧМИ).

8.2.2 ЧМИ должен представлять собой совокупность программно-технических и технических средств, различных способов представления информации операторам для реализации возможности проводить процедуры контроля и управления за технологическими процессами на АС.

8.2.3 ЧМИ должен обеспечивать эффективное взаимодействие между операторами и оборудованием/системами, обеспечивающими безопасную эксплуатацию ЭБ.

8.2.4 Для того чтобы обеспечить взаимосвязь между функциями контроля и управления, оператор должен:

– непосредственно управлять технологическим оборудованием;

– интегрировать контролирующие и управляющие функции при использовании различного оборудования/систем при нормальной эксплуатации ЭБ, включая управление при авариях.

8.2.5 Оператор, выполняющий функции интегратора по контролю и управлению технологическими процессами в различных состояниях ЭБ, должен иметь информацию, которая позволяет ему:

– оценить общее состояние ЭБ, во всех эксплуатационных условиях, то есть в режиме нормальной эксплуатации, в режиме возникновения ожидаемых при эксплуатации состояний или аварийных условий, и подтвердить того, что принимаются предназначенные для этого автоматические действия, направленные в сторону безопасности;

– определять необходимость процедур по контролю и управлению технологическими процессами.

8.2.6 В случае возникновения отклонений от нормальной эксплуатации (переходных режимов/предаварийной ситуаций/аварии), ЧМИ должен быть реализован так, чтобы вся необходимая оператору информация для контроля и управления была доступна в понятном и однозначном виде. В то же самое время, оператор не должен быть перегружен большими количествами данных, которые

могут быть им трудно воспринимаемы вследствие ограничений накладываемых на человеческие возможности восприятия, распознания, памяти и реагирования.

Необходимо особое внимание уделять уменьшению вероятности ошибок с учетом человеческого фактора.

8.2.7 Необходимо рассматривать и учитывать человеческий фактор и ЧМИ с начальной стадии разработки БПУ/РПУ, чтобы гарантировать соответствующее и ясное разграничение функций между оператором и автоматикой.

8.2.8 В начальной стадии разработки БПУ/РПУ необходимо учитывать:

– уровень/объем необходимой подготовки операторов;

– объем процедур при выполнении функций контроля и управления технологическими процессами в различных состояниях ЭБ, выполняемые операторами;

– организационный состав смены/команды, которая при использовании различных средств и управляющих систем, с использованием ЧМИ выполнит функции контроля и управления с учетом человеческого фактора, а также технических и организационных аспектов ведения технологического процесса.

8.2.9 Для реализации функций контроля и управления технологическими процессами должна использоваться система, выполняющая интегрирующие/объединяющие функции всех систем ЭБ во всех эксплуатационных состояниях учитывающая все аспекты ЧМИ.

Данные функции должна выполнять интегрирующая система контроля и управления входящая в состав управляющих систем энергоблока, важных для безопасности.

ИСКУ должна состоять из двух составных частей, выполняющих свои специфические функции и дополняющие друг друга в различных состояниях ИСКУ при эксплуатации ЭБ:

– программно-технического комплекса ИСКУ;

– технических средств оперативно-диспетчерского управления.

ПТК ИСКУ должен включать в себя ряд программно-технических средств, таких как:

– рабочие станции с различным количеством средств отображения и манипуляторами для выполнения функций контроля и управления технологическими процессами в различных состояниях ЭБ, объединенными в автоматизированные рабочие места;

– сервера;

– телекоммуникационные устройства, выполняющие связующие/ объединяющие функции между ПТС и смежными системами.

Для организации информационного обмена как внутри ПТК ИСКУ, так и для связи со смежными системами для повышения уровня помехозащищенности должны использоваться волоконно-оптические линии связи.

ТС ОДУ должны включать в себя конструктивы позволяющие расположить на них необходимые измерительные приборы различного типа, светосигнальные табло и элементы контроля и управления оборудованием различного типа (арматура, насосы, регуляторы и т.д.).

8.2.10 Интерфейсы для операторов на ЭБ с использованием элементов ИСКУ, должны быть реализованы на БПУ/РПУ.

Интерфейсы должны включать в себя средства отображения связанные с безопасностью, средства управления связанные с безопасностью, системы контроля при отклонениях от нормальной эксплуатации, предупредительную и аварийную сигнализацию, а также системы/средства позволяющие получить в хронологическом порядке необходимые данные/информацию.

8.3 Средства управления

8.3.1 Если оборудование, важное для безопасности, может управляться как с БПУ, так и с РПУ, реальное место управления следует обозначать визуальными средствами (светосигнальными табло, положением ручных выключателей).

8.3.2 При разработке средств управления необходимо предусматривать условия позволяющие выполнять функции живучести БПУ/РПУ при пожаре, землетрясении, падения самолета, несанкционированном доступе.

8.3.3 Между БПУ, РПУ и другими пунктами управления должна быть реализована связь различных видов (радио, телефонная, громкоговорящая и т.д.). Реализацию способов связи следует выполнять таким способом, чтобы отказы электрических систем или других возникающих ИС не могли приводить к отказу двух систем связи одновременно.

8.4 Средства отображения информации на РС

8.4.1 Средства отображения должны предоставлять информацию операторам о состоянии ЭБ, систем и оборудования, которую требуется контролировать, чтобы обслуживать и использовать системы, важные для безопасности и поддерживать режимы ЭБ в допустимых пределах установленных в проекте.

8.4.2 Средства отображения предназначены, чтобы выполнять следующие функции:

– информировать операторов о состоянии оборудования/технологических систем и состоянии безопасности ЭБ;

– обеспечивать информацией о состоянии параметров изменяющихся во времени, важных для безопасности, для непосредственного или последующего анализа при принятии решений необходимых для поддержания безопасных пределов и условий эксплуатации;

– обеспечивать необходимой диагностической информацией о состоянии оборудования/систем.

8.4.3 В случае изменения в состоянии систем безопасности необходимо предоставлять эту информацию оператору, в том числе используя средства отображения информации на РС.

8.4.4 В режимах нормальной эксплуатации операторы используя средства отображения информации, постоянно контролируют состояние ЭБ по набору видеокадров, включающих в себя элементы отображения и сигнализации или визуальных блоков, которые обеспечивают операторов БПУ всей необходимой информацией в доступном виде без проведения предварительного анализа.

Сигнализация различного типа (вызывная, предупредительная и аварийная) в виде определенного цветового или формообразующего кодирования на средствах отображения информации должна указывать на отклонения от нормального функционирования. Когда они возникают, операторов следует обеспечивать необходимой информацией, для того чтобы:

– идентифицировать действия, выполняемые автоматикой;

– проанализировать причину отклонения;

– контролировать дальнейшее изменение ситуации;

– выполнять любые при необходимости ручные воздействия.

8.4.5 На средствах отображения информации необходимо предоставлять все изменяющиеся параметры (аналоговые, дискретные, расчетные) с дополнительной информацией необходимой операторам для условий нормальной эксплуатации и аварийных условий. Способы представления информации (параметров) и их кодирование (формой, цветом, миганием и т.д.) на средствах отображения информации должны однозначно восприниматься операторами во всех режимах, на всех рабочих местах и пунктах управления.

8.4.6 В случаях если используется дублирование представления информации (параметров, сигнализации и т.д.) на средствах отображения информации и на ТС ОДУ, необходимо их функциональное и физическое разделение, чтобы гарантировать, что единичный отказ в системе представления не будет приводить к полной потери информации о контролируемом параметре.

8.4.7 В качестве средств отображения информации и представления операторам информации, должны использоваться цветные дисплеи/мониторы (жидкокристаллические или плазменные), допускающие возможность установки и эксплуатации на РС, входящих в состав АРМ.

8.4.8 Необходимо предусматривать возможность дублирования дисплеев/мониторов, для того чтобы избежать возможности потери части необходимой информации.

8.4.9 Каждому оператору по его выбору на дисплеях/мониторах должна быть представлена обобщенная и/или детальная информация в виде технологических

видеокадров, протоколов событий, графиков, таблиц, текстовых сообщений и дополнительной информации справочного характера.

8.4.10 Дисплеи/мониторы должны предоставлять возможность оператору получать отображение изменения любого параметра, как в графическом виде (тренда), так и в виде таблиц для анализа изменения тенденции необходимого параметра за определенный промежуток времени. Должна быть предусмотрена возможность одновременного совмещения на графике параметров различного типа (аналогового и дискретного) для их анализа и дальнейшего вывода на устройства печати.

8.4.11 Отображение недостоверных данных, обнаруженных при контроле входных сигналов и/или техническом диагностировании низовой автоматикой, должно сопровождаться четко различимым и однозначно понимаемым оператором признаком недостоверности.

8.4.12 Если в составной части системы, важной для безопасности, используемой для представления информации (параметров) имеются неисправности/отказы то, это состояние следует отображать на БПУ/РПУ.

8.4.13 Для отображения/представления информации на дисплеях/мониторах должны использоваться определенным образом структурированные видеокадры разработанные по результатам и учетом функционального анализа.

8.4.14 Отображаемая информация на видеокадрах должна быть организована в виде системы с иерархической структурой, построенной с использованием принципа «от общего - к частному».

8.4.15 Работа с видеокадрами на дисплеях должна осуществляться простыми и наглядными способами, с минимальным количеством необходимых для этого действий (с помощью отображаемых на экране кнопок или графических символов, списков видеокадров, иерархических меню, перекрестных ссылок на видеокадрах и т.п.).

8.4.16 На дисплеях должна быть реализована сигнализация (цветом, формой, миганием и т.д.) о нарушениях нормальной эксплуатации, пределов и/или условий

безопасной эксплуатации, а также о недостоверности данных и дефектах/отказах, обнаруженных при техническом диагностировании.

8.4.17 Текст сигнализации/сообщения отображаемого на дисплее должен позволять оператору однозначно определять параметр, место, время, характер и степень опасности отклонения/нарушения.

8.4.18 Сигнализация/сообщения об отклонениях/нарушениях, пределов и/или условий безопасной эксплуатации должны выдаваться даже в тех случаях, когда такие отклонения/нарушения регистрируются лишь в течение короткого времени, недостаточного для автоматического срабатывания защиты.

8.4.19 Выдача сигнализации/сообщения должна сопровождаться звуковым сигналом. При этом должна обеспечиваться селективность звуковой сигнализации в зависимости от степени опасности отклонения/нарушения (изменением частоты звука, модуляцией громкости и т.п.).

8.4.20 Оператор, который контролирует соответствующую группу отклонений/нарушений, должен иметь возможность со своего АРМ подтверждать прием каждого факта сигнализации/сообщения.

8.4.21 Подтверждение факта приема сигнализации/сообщения должно отображаться на дисплее (например, изменением цвета или частотой мигания), и вызывать отключение звукового сигнала.

8.4.22 Сигнализация/сообщение, прием которого был подтвержден, должно автоматически удаляться с экрана при исчезновении вызвавшего его нарушения.

8.4.23 Запрещение выдачи сигнализации/сообщения должно вызывать его удаление с дисплея и отключение звукового сигнала.

8.4.24 Каждая новая сигнализация/сообщение, если ее выдача ранее не была запрещена, должна немедленно отображаться на дисплее на месте прежней сигнализации/сообщения.

8.4.25 Для ввода, отображения и регистрации данных должны применяться условные обозначения (в том числе – сокращения и аббревиатуры), удобные и понятные для операторов, принятые на практике и не требующие дополнительной расшифровки или анализа.

8.5 Контроль аварийных условий

8.5.1 Необходимо обеспечить однозначность в предоставлении операторам информации о состоянии систем и оборудования ЭБ, чтобы гарантировать то, что операторы могли ее однозначно трактовать при управлении ЭБ во всех эксплуатационных условиях.

8.5.2 Представление информации необходимой для контроля и управления технологическим процессом в аварийных условиях на ЭБ следует обеспечивать на БПУ и, по мере необходимости, в дополнительных пунктах управления.

8.5.3 При определении, какая информация должна быть представлена на АРМ различных операторов, в рассмотрение следует принимать следующее:

– распознавание и понимание отклонений от условий НЭ (достижение различных уставок);

– распределение информации по принадлежности к определенным АРМ для снижения информационной нагрузки;

– идентификацию конкретной ситуации/аварии и, где возможно, определение исходного события вызвавшего отклонение;

– проверку того, что требуемые функции, направленные в сторону безопасности выполняются;

– контролировать развитие события или аварии с проведением анализа направленного на миниминизацию последствий;

– решать информационные конфликты, которые могут возникать как результаты избыточности каналов отображения.

8.5.4 Средства для выполнения функций аварийного контроля на БПУ/РПУ должны быть разработаны таким образом, чтобы позволить оператору подтвердить что:

– реактор остановлен и находится в подкритичном состоянии;

– остаточное тепловыделение отводится от активной зоны к конечному поглотителю;

– все барьеры безопасности выполняют проектные функции.

Параметры, которые должны контролироваться операторами для такого подтверждения следует выбирать на стадии разработки ЭБ.

8.5.5 Должны быть предусмотрены технические решения, препятствующие вмешательству операторов в действия, связанные с технологическими защитами и блокировками, направленными на выполнение функций безопасности, в течение 10-30 мин. после выдачи команды технологической защиты/блокировки в части систем безопасности.

8.5.6 Оборудование для контроля аварийных условий должно быть работоспособным в окружающей среде после аварии в течение необходимого периода времени. Диапазоны измерения выбранных параметров для контроля аварийных условий должны иметь более широкие границы по сравнению с аналогичными диапазонами для систем НЭ.

8.5.7 Представление операторам информации, которая используется для контроля состояния ЭБ после аварии, должно отличаться от других видов представления (формой, размером, цветом и т.д.).

8.5.8 Хронологическая информация для анализа аварии или чрезвычайных мер должна регистрироваться, храниться и использоваться для дальнейшего анализа с использованием специальных средств (например типа «черный ящик»).

8.5.9 Должны быть предусмотрены процедуры, позволяющие выдавать на ТС ОДУ систем безопасности однозначную информацию, возникающую в случае нарушений/аварий вследствие работы автоматики без воздействия операторов.

8.5.10 Все средства ручного воздействия, отображения данных, элементы индикации и органы ручного управления должны быть четко идентифицированы и расположены так, чтобы обеспечить удобство доступа к ним при необходимости, а также при техническом обслуживании и восстановлении в случае ремонта (замене отказавших изделий или их составных частей).

8.5.11 Средства прямого ручного воздействия такие как кнопки аварийной защиты, предупредительной защиты, ускоренной предупредительной защиты, запуска каналов безопасности должны быть защищены от ложного/случайного воздействия, а также иметь отличительную окраску и располагаться так, чтобы

оператор безошибочно мог выполнить действия направленные в сторону обеспечения безопасности.

8.5.12 Операторам должна быть представлена необходимая информация о техническом состоянии оборудования выполняющего функции безопасности, в том числе об отказавших и/или преднамеренно выведенных из работы независимых резервированных каналах.

8.5.13 Участие операторов в выполнении функций безопасности (инициирование, дублирование, прекращение автоматически выполняемых защитных действий, возврат УСБ в исходное состояние, а также дистанционное управление технологическими системами безопасности) должно, как правило, ограничиваться теми действиями, которые можно полностью осуществлять на БПУ/РПУ.

8.6 Система сигнализации

8.6.1 Система, реализующая функции сигнализации аварийной или предупредительной (визуальной и звуковой), а также вызывной должны привлекать внимание операторов и способствовать инициации их действий для необходимого уровня вмешательства, чтобы гарантировать то, что состояние ЭБ поддерживается в установленных проектом пределах.

8.6.2 Система сигнализации в виде светосигнальных табло с различным цветовым или формообразующим решением, а также звуковая, с использованием различных типов звучания должна реализовываться с учетом эргономических требований и определенных АРМ по принадлежности для возможности выполнения действий операторами.

8.6.3 При разработке системы сигнализации, наибольшее внимание должно быть уделено тому, чтобы важная информация могла однозначно восприниматься и распознаваться операторами, особенно в случае возникновения отклонений от НЭ и аварийных событий, которые могут инициировать большое количество сигнализации и в том числе вызывной, предупредительной и аварийной. Необходимо использовать различные способы, включая группирование

светосигнальных табло по приоритетам и создание условий сигнализации, а также, использования звукового или визуального распределения, чтобы иметь возможность разделения сигнализации различных типов и приоритетов.

8.6.4 Использование светосигнальных табло или звука должно позволять оператору своевременно идентифицировать отклонение от НЭ или аварию как отдельно, или в группах сигналов.

8.6.5 Звуковая сигнализация должна использоваться для привлечения внимания оператора при появлении новых отклонений. Необходимо использовать средства для снятия/квитирования звуковых сигналов, чтобы избегать слуховой перегрузки и облегчать идентификацию вновь появившихся сигналов, которые могут появляться впоследствии изменения ведущегося технологического процесса.

Если звуковой сигнал можно снять/квитировать, то визуальные признаки сигнализации (наличие активного табло) следует оставлять до тех пор, пока не будет выяснена первопричина отклонения/отказа. Визуальные средства (изменение цвета или изменение частоты мигания) необходимо использовать, для того чтобы отличить условия сигнализации, которые были подтверждены от условий сигнализации, которые еще не были подтверждены/квитированы, оператором. Когда состояние оборудования/системы вернется к нормальному, индикацию сигнализации следует сохранять до тех пор, пока ее не снимет оператор, чтобы сохранить информацию об имевшемся отклонении/отказе.

8.7 Системы регистрации хронологических данных

8.7.1 Должна быть предусмотрена возможность создания архивов для регистрации, хранения и получения для анализа данных о состоянии параметров и оборудования/систем ЭБ в любых режимах и в любой момент времени, используя которые в результате проведения необходимого анализа можно представить процесс протекания того или иного события.

Такие архивы должны предоставлять операторам:

– информацию из текущих архивов (предоставление в графическом и табличном виде) за определенные интервалы времени, например – 5 мин, 10 мин, 30 мин и т.д.;

– информацию из долговременных архивов (предоставление в графическом и табличном виде) за выбранные оператором промежутки времени.

8.7.2 Необходимо предусматривать на БПУ/РПУ и в других местах определяемых проектом, наличие устройств которые позволяют получать распечатки (бумажные копии) архивов, копий экранов, отчетов и т.д. для их дальнейшего использования. Устройства должны обеспечивать печать различных форматов (А3, А4) в цветном исполнении.

8.7.3 Доступ к архивам должен предоставляться операторам на БПУ/РПУ с использованием единого интерфейса.

При разработке интерфейса работы с архивной информацией необходимо учитывать обязанности операторов, затраты времени для получения информации и удобство пользования.

9 Полигонные испытания. Общие технические требования

9.1 Общие сведения

Опыт эксплуатации УСВБ, создаваемых «проектным» путем показывает, что, как правило, они не удовлетворяют техническим требованиям, точностным, динамическим и надежностным характеристикам, приведенным в Техническом задании на систему. При этом бывают плохо проработаны вопросы стыковки управляющих систем с интегрирующей системой контроля и управления, не оптимально решены вопросы интерфейса «человек – машина», неудовлетворительно решены вопросы эксплуатации и т.д. Эксплуатация и обслуживание таких систем трудоемка и неэффективна.

Устранить указанные выше недостатки возможно путем организации комплексных полигонных испытаний систем и комплектной поставки технических и программно-технических средств, входящих в состав систем, как продукции производственно-технического назначения.

9.2 Условия проведения комплексных полигонных испытаний

9.2.1 Проведение комплексных полигонных испытаний средств и управляющих систем, важных для безопасности возможно при выполнении следующих условий:

– завершено выполнение строительных и отделочных работ помещений Полигона;

– подготовлены и введены в работу все обеспечивающие системы, в том числе:

а) вентиляции;

б) кондиционирования;

в) пожаротушения;

г) защитного и специального заземления;

д) связи;

е) освещения;

ж) электроснабжения и т.д.

– персонал Полигона укомплектован, обучен и прошел проверку знаний в установленном порядке;

– разработана эксплуатационная документация, необходимая для проведения испытаний;

– определены и согласованы в установленном порядке:

а) перечень исходных событий аварий для оборудования и систем энергоблока, а также оборудования и программного обеспечения, входящих в состав системы;

б) состав испытуемого оборудования, функций и задач системы;

в) перечень режимов работ (режимы нормальной эксплуатации, режимы с нарушением условий нормальной эксплуатации, переходные режимы) энергоблока, включая предаварийные и аварийные, при которых будет испытана система;

г) перечень диагностируемых событий в работе энергоблока, основного технологического и электрического оборудования, а также оборудования систем контроля, управления, защит, надежного электроснабжения и действий оператора;

д) массивы входной информации для имитации технологических процессов и работы оборудования энергоблока, диагностируемых событий и проверки алгоритмов информационной поддержки оператора;

– разработаны и согласованы в установленном порядке Планы-графики, программы и методики проведения испытаний;

– подготовлен и введен в работу инструментально-испытательный комплекс Полигона, в том числе средства измерения, испытательное оборудование, имитаторы и математические модели, используемые для испытания системы, при этом указанные средства должны иметь соответствующий класс и обеспечивать необходимую точность измерений;

– разработана, изготовлена, поставлена и введена в работу представительная часть, либо поставочный комплект технических и программно-технических средств испытываемой системы.

9.2.2 Непременным условием поставки технических и программно-технических средств системы на Полигон является выполнение требований о проведении предварительных автономных стендовых испытаний системы на предприятиях-зазработчиках и заводах-изготовителях, о чем должна быть сделана соответствующая запись в формуляре (паспорте) на указанные средства и представлены протоколы и акты их испытаний.

9.2.3 При проведении испытаний на представительной части технических и программно-технических средств системы обязательным условием является наличие разработанного и согласованного с Генеральным проектировщиком и одобренного Ростехнадзором обоснования представительности, дающего возможность распространить результаты полигонных испытаний на поставочный комплект технических и программно-технических средств системы.

9.2.4 В случае отсутствия на предприятиях-разработчиках и заводах-изготовителях специальных комплексных стендов для проведения предварительных автономных испытаний технических и программно-технических средств в составе системы, допускается предварительные автономные испытания этих систем провести на Полигоне перед комплексными испытаниями всей системы.

9.2.5 Испытания системы должны начинаться только после того как на Полигоне завершены все подготовительные работы, налажены и испытаны интерфейсы связи с подсистемами, налажено и опробовано общее функционирование системы, о чем должен быть составлен соответствующий акт.

9.2.6 До начала проведения комплексных полигонных испытаний Приемочной комиссии должна быть представлена для рассмотрения следующая техническая и организационная документация:

– приказ о назначении Приемочной комиссии;

– программы, методики, акты и протоколы испытаний оборудования и подсистем на предприятиях разработчиков системы и заводах-изготовителях, формуляры (паспорта) на указанное оборудование;

– акты и протоколы готовности полигона, обеспечивающих систем, комплекса технических и программно-технических средств системы к проведению испытаний;

– план-график, программы и методики проведения испытаний системы;

– оперативная эксплуатационная документация;

– акты, протоколы о готовности инструментально-испытательного комплекса, в том числе измерительного, испытательного оборудования, средств, имитаторов и математических моделей;

– технические задания на систему и Полигон;

– технические Проекты на систему и Полигон;

– техническая документацию на комплекс технических и программно-технических средств и программное обеспечение системы.

9.2.7 По результатам рассмотрения перечисленных выше документов, а также фактической готовности Полигона и комплекса технических и программно-технических средств системы к проведению комплексных испытаний, Приемочная комиссия выдает разрешение на проведение испытаний.

9.3 Цели и критерии оценки комплексных полигонных испытаний

9.3.1 Испытания должны проводится в соответствии с программами и методиками, содержащими требования, условия и значения технических

характеристик, которые указываются в проектной документации на систему, при условии, что для испытания были выполнены все предварительные условия, соблюдены соответствующие внешние условия испытаний.

9.3.2 Основными целями комплексных полигонных испытаний системы является проверка:

– взаимодействия комплекса технических и программных средств системы в реальном масштабе времени для выполнения предусмотренных проектной документацией критериев качества функционирования системы;

– функционирования отдельных ПТС в рамках системы, а также интерфейсов связи с ИСКУ, в том числе:

а) основных временных характеристик каналов передачи данных системы, в том числе скоростей передачи данных;

б) устойчивости каналов передачи данных к изменению информационной загрузки;

в) функционирования и точности системы единого времени;

г) временных характеристик системы при различной загрузке сетевых средств / каналов передачи данных;

– выполнения отдельных функций, групп взаимосвязанных функций и системы в целом;

– основных временных характеристик системы;

– работоспособности резервированных структур;

– эксплуатационных характеристик оборудования и системы в целом;

– технологии технического обслуживания системы в процессе эксплуатации с учетом выполнения проектного «Регламента технического обслуживания» системы в процессе эксплуатации энергоблока»;

– выполнения требований нормативно-технической документации по безопасности к функционированию и эксплуатации системы;

– технологии ведения монтажа и наладки системы на объекте с выработкой соответствующих рекомендаций;

– функционирования системы в условиях структурной и функциональной деградации, контроля достоверности, помехозащищенности и надежности комплекса программного обеспечения системы;

– влияния на безопасную и надежную эксплуатацию энергоблока функционирования программно-технических комплексов в условиях наличия алгоритмических, программных сбоев и отказов;

– отработки системой проектных алгоритмов при работе энергоблока в переходных, стационарных, динамических и аварийных режимах работы, а также проектных исходных событий аварии;

– отработки системой проектных алгоритмов при наличии единичных отказов в системе, в том числе и по общей причине;

– отработки системой проектных алгоритмов при наличии одного из учитываемых проектом исходного события с наложением одного независимого от исходного события неконтролируемого отказа элемента системы, которые могут влиять на развитие аварии и привести к нарушению пределов безопасной эксплуатации;

– функционирования системы в условиях отказа обеспечивающих систем;

– устойчивости контуров регулирования и управления во всех проектных режимах работы энергоблока, в том числе устойчивости работы энергоблока в условиях действия предусмотренных проектном систем регулирования, управления, защит и блокировок;

– эффективности идентификации системой уровня безопасности энергоблока в текущий момент времени;

– эффективности и удобства эксплуатации интерфейса «человек – машина»;

– метрологического обеспечения системы;

– эффективности алгоритмов идентификации событий и отказов в работе энергоблока, основного технологического и электротехнического оборудования, ошибочных действий оператора (в соответствии с перечнем диагностируемых событий);

– эффективности системы диагностики и алгоритмов идентификации неисправностей и отказов в работе оборудования системы, используемых программных средств и системы в целом;

– эффективности алгоритмов экспертной информационной поддержки оператора;

– обеспечения контроля и управления механизмами и оборудованием энергоблока с БПУ и РПУ;

– характеристик и эффективности системы регистрации важных параметров эксплуатации, а также алгоритмов сохранения и восстановления информации при аварийных ситуациях, неисправностях в работе системы, включая отказы по общей причине;

– алгоритмов автоматического и автоматизированного пуска и расхолаживания основных технологических агрегатов и энергоблока в целом.

– эффективности алгоритмов и средств документирования и анализа хода технологического процесса (включая аварийные ситуации), а также действий оператора по управлению энергоблоком и системой;

– технических решений по обеспечению пожарной безопасности системы;

– эффективности технических средств управления запроектными авариями;

– специальных методик и программ по определению и продлению назначенных показателей оборудования и системы в целом, а также автоматизированной оценки ресурса работы оборудования;

– алгоритмов и программ распознавания предаварийных ситуаций с оценкой путей их возможного развития;

– оптимизации численности обслуживающего персонала, трудозатрат на монтаж и наладку системы;

– управления радиационной обстановкой на АС и окружающей среды;

– верификация программного обеспечения системы и определение условий и требований к его тиражированию.

При этом должны оцениваться качественные и количественные характеристики выполняемых функций, выявляются возможности совместных действий всех функциональных групп системы.

Особое внимание при этом следует обратить на определение разрешающей способности, точностных и динамических характеристик каналов связи системы в целом в условиях высокой частоты запросов, большого объема входной и выходной информации.

9.3.3 Критериями комплексных полигонных испытаний средств и систем, важных для безопасности являются:

– получение количественных и качественных характеристик оборудования, интерфейсов связи и системы в целом, удовлетворяющих эксплуатационным / технологическим требованиям, требованиям технического задания и нормативно-технической документации по безопасной эксплуатации АС;

– подтверждение проектных свойств аппаратных и программных средств системы сохранять в заданных экстремальных условиях эксплуатации гарантированный объем функций контроля и управлению энергоблоком;

– подтверждение проектных свойств отказоустойчивости системы;

– подтверждение показателей качества функций защит блокировок и управления системами безопасности;

– подтверждение реализации информационной поддержки оператора в переходных и аварийных режимах работы энергоблока;

– предотвращение выдачи программно-техническими комплексами ложных управляющих воздействий в условиях наличия электромагнитных помех и наводок напряжения;

– подтверждение наличия проектной блокировки неправильных действий персонала;

– подтверждение реализации в системе функций диагностики основного технологического, электротехнического оборудования, а также аппаратных и программных средств системы, прогнозирование хода технологического процесса станции.

– предварительно оцененный научно-технический уровень системы, удовлетворяющий современным требованиям аналогичных систем ведущих стран.

9.4 Требования к содержанию программ и методик комплексных испытаний

9.4.1 Содержание программ и методик комплексных полигонных испытаний системы должны отвечать требованиям ГОСТ 34.603, РД 50-34.698 с учетом положений ГОСТ 2.105, а также требованиям настоящего раздела.

9.4.2 В программах и методиках испытаний должны быть формы протоколов и актов испытаний.

9.4.3 План-график проведения комплексных полигонных испытаний системы, состав программ и методик испытаний должны определять весь спектр необходимых испытаний, очередность, порядок проведения и действия персонала в процессе испытаний, требования к документальному оформлению испытаний, критерии приемлемости результатов испытаний с тем, чтобы можно было идентифицировать системные, технические, эксплуатационные и эргономические характеристики системы и убедиться, что комплекс технических и программно-технических средств создаваемой системы обеспечит надежное и качественное выполнение заданных системных функций по безопасному управлению энергоблоком во всех проектных режимах его работы.

9.4.4 Перечень проверяемых функций и задач определяется техническим заданием на систему. В дополнении к изложенному выше в программы и методики испытаний функций и задач системы должны быть включены следующие испытания (проверки):

– функционирования системы при отклонениях напряжения электропитания по амплитуде и частоте в пределах требований технических условий на технические и программно-технические средства и ТЗ на систему;

– функционирования технических и программно-технических средств при выполнении АВР по электропитанию и с перерывом электропитания, допускаемым техническими условиями на оборудование и техническим заданием на систему, в

том числе и с имитацией промышленных помех, возникающих в питающих систему электросетях;

– помехозащищённости технических и программно-технических средств системы и возможности подавления электромагнитных помех во входных цепях и восстановления программной информации;

– достоверности функционирования программного обеспечения системы при наличии сбоев, отказов, зацикливаний, искажений информации в оперативных запоминающих устройствах, в том числе диагностики программного обеспечения системы;

– проверка программных средств идентификации санкционированных пользователей;

– проверка защиты от несанкционированного доступа, реализованной в устройствах, обеспечивающих неоперативное изменение уставок;

– ремонтопригодности и удобства обслуживания оборудования системы, в том числе обеспечение возможности замены отдельных блоков, устройств, электронных модулей и плат в работающем оборудовании без последующей подстройки и нарушения пределов и условий безопасной эксплуатации энергоблока;

– безопасного функционирования оборудования и системы в целом при имеющихся многоцелевых проектных совмещениях элементов и устройств при единичных отказах, а также и отказах по общим причинам;

– эффективности устройств и приспособлений для периодических и послеремонтных прямых и полных проверок системы на соответствие проектным характеристикам;

– эффективности устройств и приспособлений для проверки работоспособности и правильности функционирования системы в процессе эксплуатации;

– устройств и приспособлений для проверки времени и последовательности прохождения сигналов и включения оборудования, в том числе и переход на аварийные источники электропитания;

– возможности безопасного исполнения и эффективности проектного «Регламента технического обслуживания» в процессе эксплуатации системы;

– эффективности средств исключающих (или ослабляющих) единичные ошибки персонала, в том числе при техническом обслуживании оборудования системы;

– поведение системы (реакция системы) на возможные схемные и программные неисправности в процессе эксплуатации, в том числе короткие замыкания, потеря качества изоляции, наводки и посадки напряжения, искажение данных и нарушение вычислительного процесса, зацикливание, сбои, отказы, потеря исходных данных в оперативном запоминающем устройстве, искажение заданной последовательности вызовов и т.д.);

– выявление опасных и ложных реакций оборудования и системы в целом;

– оперативной оценки персоналом состояния с соблюдением пределов и условий безопасной эксплуатации энергоблока и системы, в том числе идентификации текущего уровня безопасной эксплуатации энергоблока.

– безопасного и несанкционированного ввода / вывода защит и блокировок энергоблока, изменения их установок в процессе эксплуатации;

– технических мер, исключающих ложное срабатывание защит и блокировок энергоблока;

– технических мер, исключающих возможность утраты зарегистрированной информации и несанкционированного, доступа к устройствам, базам данных, архивам системы, в которых зафиксированы технологические данные энергоблока до и после срабатывания защит.

– УСБ в части обеспечения:

а) формирования сигналов «Готовность УСБ» и «Неисправность УСБ» при любом единичном отказе технических и программно-технических средств системы;

б) дистанционный и ручной запуск системы, путем воздействия на один элемент (ключ, кнопка и т.д.);

в) доведения до конца начавшегося действия системы;

г) поканальной проверки работоспособности системы в процессе эксплуатации;

д) технических мер, препятствующих вмешательству оператора в действия системы в течении установленного времени;

е) исключения ложных срабатываний системы;

ж) самодиагностики состояния системы в процессе эксплуатации;

– достоверности функционирования контуров управления, регулирования и защиты в условиях программных сбоев и отказов;

– обеспечивающих систем (по отдельным программам).

9.4.5 Все изменения, вносимые в программы и методики, как и изменения объема испытаний системы, должны рассматриваться комиссией и согласовываться в установленном порядке с предприятиями и организациями, участвующими в проведении испытаний.

9.5 Организация и проведение комплексных полигонных испытаний

9.5.1 К комплексным испытаниям на Полигоне допускается средства и УСВБ:

– проектная и конструкторская документация на которые согласована и утверждена в установленном порядке;

– конструирование и изготовление оборудования, изделий и подсистем выполнено на предприятиях, имеющих соответствующие лицензии;

9.5.2 Предприятия поставщики обязаны осуществлять комплектную поставку, предварительно испытанного на стендах заводов изготовителях или головного предприятия оборудования, изделий и подсистем.

9.5.3 План-график проведения испытаний, программы и методики комплексных полигонных испытаний системы должны быть согласованы с предприятиями и организациями членами Приемочной комиссии и утверждены Заказчиком системы.

9.5.4 Руководство и координация комплексными полигонами испытаний средств и УСВБ осуществляет Приемочная комиссия, назначенная приказом.

9.5.5 По согласованию и необходимости в состав комиссии следует включить представителей Заказчика системы, Главного конструктора РУ, Генпроектанта АС, заводов-изготовителей и др.

9.5.6 Для оперативного выполнения работ по испытанию оборудования и функций системы, Председатель Приемочной комиссии своим распоряжением

назначает Руководителя испытаний и его заместителей по технической и программной части, рабочие группы, руководителей этих групп и устанавливает график их работ.

9.5.7 Рабочие группы в своей деятельности руководствуются разработанными и согласованными программами и методиками испытаний, планом - графиком проведения испытаний, документацией на комплекс технических и программно-технических средств, техническими проектами и заданиями на систему и Полигон, результатами стендовых заводских испытаний, документацией на инструментально-испытательный комплекс, в том числе контрольное, испытательное оборудование, имитаторы, модели и техническими распоряжениями руководителя испытаний.

9.5.8 В процессе испытаний рабочие группы (руководители) ведут систематическую запись обо всех своих действиях и результатах испытаний в «Оперативном журнале испытаний». О возникающих в процессе испытаний системных дефектах и неполадках в работе технических и программно-технических средств, а также предложениях по совершенствованию оборудования, программ и методик испытаний – в «Журнале дефектов и предложений».

9.5.9 Все вопросы, возникающие в процессе испытаний, Руководители рабочих групп оперативно решают с Руководителем испытаний.

9.5.10 Для оформления результатов испытаний должны быть предварительно разработаны формы протоколов и актов испытаний. Указанные протоколы и акты оформляются на каждую испытываемую функцию системы и каждую задачу специального математического обеспечения с обязательным приложением распечаток ЭВМ и выводом о соответствии проверяемой функции (задачи) требованиями ТЭ и ТП.

Целесообразно максимально автоматизировать процесс проведения испытаний системы (запоминания, распечатки и обработки результатов испытаний).

9.5.11 Должны быть определены условия, при которых требуются повторение испытаний.

9.5.12 Все зафиксированные при испытаниях дефекты и неполадки должны быть проанализированы, определены их причины и намечены пути устранения.

9.5.13 На основании отдельных протоколов и актов испытаний каждой функции системы, ее задач, записей в оперативных журналах испытаний оформляется общий «Акт комплексных полигонных испытаний системы». Акт подписывается членами Приемочной комиссии и утверждается Заказчиком системы. В содержании указанного акта должны найти отражения:

– основные результаты испытания системы с выводами о соответствии (не соответствии) технических характеристик системы требованиям технического задания, технологическим требованиям, а также требования нормативно-технической документации по безопасности;

– качество выполняемых функций и задач системой;

– заключение о возможности надежного и безопасного управления энергоблоком во всех проектных режимах эксплуатации;

– заключение о возможности поставки технических и программно-технических средств системы на АС;

– рекомендации по доработке технических, программно-технических и программных средств системы, а также дополнительных испытаниях, в том числе и на заводах-изготовителях;

– оценка эффективности и рекомендации по доработке инструментально-испытательного комплекса, в том числе имитаторов и моделей;

– предварительная оценка научно-технического уровня системы.

9.5.14 По результатам комплексных полигонных испытаний системы организацией разработчиком системы в трехмесячный срок оформляется технической отчет.

10 Монтаж средств автоматизации управляющих систем

10.1 Общие требования

10.1.1 Настоящий раздел устанавливает общие требования к организации, производству и приемке работ по монтажу средств автоматизации, программно-технических средств и/или программно-технических комплексов, далее по тексту средства автоматизации, на АС (энергоблоке АС).

10.1.2 Монтажные организации, привлекаемые к выполнению работ по монтажу средств автоматизации на АС (энергоблоке АС), должны иметь лицензии Ростехнадзора на право производства работ и оказания услуг, по заявленному виду деятельности, на объектах атомной энергетики;

10.1.3 Эксплуатирующей организацией должны быть определены монтажная и наладочная организации осуществляющие техническое руководство работами по монтажу и наладке средств автоматизации на АС (энергоблоке АС).

10.1.4 Монтажной и наладочной организациями должен быть разработан, согласован (с заинтересованными организациями) и утвержден эксплуатирующей организацией, организационно-распорядительный документ, определяющий зоны разграничения ответственности, порядок взаимодействия между организациями на стадии монтажа и предпусковых наладочных работ на АС (энергоблоке АС).

10.1.5 С целью регламентации деятельности по обеспечению качества, направленной на реализацию основных критериев и принципов обеспечения безопасности АС, монтажными организациями, выполняющими работы и предоставляющими услуги эксплуатирующей организации АС, должны быть разработаны частные программы обеспечения качества в рамках ПОК АС (С) Генерального подрядчика по строительству АС (энергоблока АС).

10.1.6 Работы по монтажу средств автоматизации должны проводиться в соответствии с графиком выполнения электромонтажных работ, утвержденной проектно-сметной документацией, проектом производства работ, рабочей проектной документацией, а также в соответствии с технической документацией предприятий-изготовителей средств автоматизации, с соблюдением федеральных норм и правил, действующих в атомной энергетике.

10.2 Подготовка к производству монтажных работ

10.2.1 В составе общей организационно-технической подготовки должны быть определены и согласованы эксплуатирующей организацией (заказчиком) и монтажной организацией:

– условия комплектования объекта первичными измерительными преобразователями, приборами, изделиями и материалами поставки заказчика, не входящими в комплект поставки СКУ;

– условия комплектования изделиями и материалами, инструментом и приспособлениями поставки подрядчика - монтажной организации;

– перечень средств автоматизации, монтаж которых выполняется под техническим контролем представителей предприятий-изготовителей;

– условия транспортирования кабельной продукции, щитов, пультов, ПТС / ПТК, трубных блоков к месту монтажа.

10.2.2 При подготовке монтажной организации к работам по монтажу средств автоматизации должны быть выполнены следующие этапы:

– получена проектная документация и документация предприятий-изготовителей средств автоматизации;

– выполнена проверка полноты и качества представленной документации, на возможность выполнения монтажа, включая критерии приемки;

– разработаны мероприятия по подготовке и поддержанию квалификации персонала, в том числе руководителей и специалистов;

– выполнена подготовка, проверка знаний и аттестация персонала осуществляющего работы по монтажу средств автоматизации (включая контролеров служб технического контроля);

– разработан и утвержден ППР;

– разработаны и согласованы с заводами-изготовителями и эксплуатирующей организацией технологические карты на монтаж средств автоматизации;

– выполнен входной контроль технологической оснастки, технических средств, для транспортировки, установки, сборки и монтажа средств автоматизации, произведена их выдача в производство, решены вопросы по обеспечению исправного состояния средств автоматизации при производстве работ;

– выполнен входной контроль, настройка, поверка приборов и средств контроля качества работ, определено их использование по назначению и содержанию при производстве работ;

– произведена приемка строительной и технологической готовности объекта к монтажу средств автоматизации (включая скрытые работы);

– произведена приемка оборудования (первичных измерительных преобразователей, приборов, щитов, пультов, ПТС / ПТК и т.п.), изделий и материалов от заказчика и генподрядчика:

– произведена укрупнительная сборка узлов и блоков;

– выполнены предусмотренные нормами и правилами мероприятия по охране труда и противопожарной безопасности.

10.2.3 До начала монтажа средств автоматизации, монтажной организацией совместно с Генподрядчиком на строительство АС и Заказчиком должны быть решены следующие вопросы:

– установлены и согласованы опережающие сроки строительства специальных помещений (предназначенных для средств автоматизации) обеспечивающих своевременное проведение индивидуальных испытаний вводимых в действие технологических систем АС (энергоблока АС);

– определены технологические системы энергоблока АС и сроки их передачи под индивидуальные испытания после выполнения монтажа средств автоматизации;

– предусмотрены необходимые производственные мастерские, бытовые и производственные помещения, оборудованные отоплением, вентиляцией, освещением, средствами связи и оргтехникой;

– предусмотрено использование основных строительных машин, находящихся в распоряжении Генподрядчика (транспортных средств, подъемно-разгрузочных машин и механизмов и т. п.), для перемещения крупногабаритных узлов (блоков щитов, пультов, труб и т. п.), от складских помещений Заказчика и от производственных баз монтажных организаций, до установки их в проектное положение на площадке АС (энергоблока АС);

– разработаны рекомендации и схемы подъема крупногабаритных узлов на проектные отметки и их перемещение через монтажные проемы;

– предусмотрены постоянные или временные сети, подводящие к объектам электроэнергию, воду, сжатый воздух, с устройствами для подключения оборудования и инструмента;

– предусмотрены в соответствии с требованиями документации предприятий-изготовителей, мероприятия по обеспечению защиты средств автоматизации (щитов, пультов, трубных, электрических проводок и т.п.) от влияния атмосферных осадков, грунтовых вод, низких температур, от загрязнения и повреждений, а ПТС / ПТК от статического электричества.

10.2.4 В рабочей документации на средства автоматизации, принимаемой к производству работ, монтажная организация должна проверить:

– соответствие рабочей документации на средства автоматизации технологической, электротехнической, сантехнической и другой рабочей документацией;

– привязки в рабочих чертежах ПИП, приборов и средств автоматизации, поставляемых предприятиями-изготовителями комплектно с технологическим оборудованием;

– учет требований высокой заводской и монтажной готовности оборудования, максимального переноса трудоемких работ в монтажно-заготовительные мастерские;

– указания категорий трубных и импульсных проводок в проектной документации;

– наличие взрывоопасных или пожароопасных зон и их границы, категории, группы и наименования взрывоопасных смесей; места установки разделительных уплотнений и их типы.

Все выявленные несоответствия в рабочей документации должны передаваться разработчику по акту. Все изменения в рабочую документацию должны быть внесены до начала электромонтажных работ.

10.2.5 Приемку строительной и технологической готовности объекта к монтажу средств автоматизации следует осуществлять поэтапно по отдельным

законченным частям объекта (помещения щитового оборудования, помещения ПТС / ПТК, помещения первичных измерительных преобразователей и т. п.).

10.2.6 Поставка на объект изделий и материалов организацией, монтирующей оборудование, средств автоматизации / ПТС / ПТК, должна осуществляться, как правило, с помощью контейнеров.

10.3 Приемка объекта под монтаж

10.3.1 До начала монтажа средств автоматизации на строительной площадке АС, а также в зданиях и помещениях, сдаваемых под монтаж средств автоматизации, должны быть выполнены строительные работы, предусмотренные рабочей документацией и проектом производства работ.

В строительных конструкциях зданий и сооружений (полах, перекрытиях, стенах, фундаментах оборудования) в соответствии с архитектурно-строительными чертежами должны быть:

– нанесены разбивочные оси и рабочие высотные отметки;

– установлены закладные конструкции под щиты, пульты, ПТС / ПТК и т. п. в соответствии с проектной документацией и документацией заводов-изготовителей;

– выполнены каналы, туннели, ниши, борозды, закладные трубы для скрытой проводки, проемы для прохода трубных, импульсных и электрических проводок с установкой в них коробов, гильз, патрубков, обрамлений и других закладных конструкций;

– установлены площадки для обслуживания ПИП, отборных устройств, уравнительных сосудов, приборов и арматуры;

– оставлены монтажные проемы для перемещения крупногабаритных узлов и блоков.

10.3.2 В помещениях и местах, предназначенных для монтажа средств автоматизации, должны быть закончены строительные и отделочные работы, произведена разборка опалубок, строительных лесов и подмостей, не требующихся для монтажа средств автоматизации.

10.3.3 До начала монтажа кабельных проводок, в кабельных сооружениях и производственных помещениях должны быть:

– закончены в проектном объеме строительные работы и выполнена гидроизоляция;

– выполнены работы по нанесению огнезащитного покрытия стен и металлоконструкций;

– выполнены работы по опережающему вводу установок пожаротушения;

– выполнены работы по вводу в работу штатного освещения для кабельных сооружений и сданы по акту заказчику;

– оборудованы посты с первичными средствами пожаротушения;

– назначены приказом, по эксплуатирующей и монтажной организации, лица ответственные за противопожарное состояние конкретных кабельных сооружений и эксплуатацию установок пожаротушения;

– разработаны, согласованы и утверждены инструкции по действиям эксплуатационного персонала, монтажных и наладочных организаций в случае возникновения пожара.

10.3.4 Помещения, предназначенные для средств автоматизации, должны быть оборудованы отоплением, вентиляцией, при необходимости кондиционированием, смонтированными по постоянной схеме, иметь дверные запоры. Также должны быть выполнены магистрали заземления в соответствии с проектом и требованиями ПУЭ.

10.3.5 В помещениях, предназначенных для средств автоматизации, должно быть выполнено рабочее, аварийное и эвакуационное освещение, а также защита осветительной сети в соответствии проектной документацией и требованиями ПУЭ. Выполнение работ должно быть подтверждено протоколом испытаний и актом принятия в эксплуатацию осветительной сети. Закончен монтаж технических средств системы пожаротушения.

10.3.6 На дверях помещений должны быть нанесены знаки категорий помещений по пожарной, электрической и взрывоопасности в соответствии с проектом и требованиями НПБ 160, ПУЭ.

10.3.7 После сдачи указанных помещений под монтаж систем автоматизации в них не допускается производство строительных работ и монтаж санитарно-технических систем.

10.3.8 В помещениях предназначенных для монтажа ПТС / ПТК в дополнение к требованиям 11.3.4, должно быть выполнено заземление и экранирование помещений, обеспечено поддержание микроклимата в соответствии с проектными требованиями.

10.3.9 Приемка указанных помещений осуществляется:

– при соответствии протокола по проверки кондиционирования воздуха в помещениях (с оценкой содержания в воздухе хлоридов, сульфатов и сернистого газа) проектным требованиям;

– при наличии протокола проверки экранирования помещения на соответствие требованиям, указанным в проектной документации и документации заводов-изготовителей ПТС / ПТК;

– при наличии протокола проверки выполненного заземления и/или специального заземления в помещении ПТС / ПТК, на соответствие требованиям проектной документации и документации заводов-изготовителей, в том числе и в герметичной оболочке;

– при наличии протоколов подтверждающих обеспечение пожарной безопасности в помещениях ПТС / ПТК;

– при наличии протоколов подтверждающих обеспечения защиты от несанкционированного доступа в помещения ПТС / ПТК.

В данных помещениях, при монтаже технических средств / ПТС / ПТК должен поддерживаться микроклимат в соответствии с требованиями проекта.

На окнах должны быть предусмотрены средства защиты от прямых солнечных лучей (жалюзи, шторы).

10.3.10 К началу монтажа средств автоматизации на технологическом оборудовании и других видах оборудования, на трубопроводах должны быть установлены:

– закладные и защитные конструкции для монтажа первичных измерительных преобразователей. Закладные конструкции для установки отборных устройств давления, расхода и уровня должны заканчиваться запорной арматурой;

– первичные измерительные преобразователи и средства автоматизации, встраиваемые в трубопроводы, воздуховоды и аппараты (сужающие устройства, диафрагмы, ротаметры, проточные датчики расходомеров и концентратомеров, уровнемеры всех типов, регулирующие органы и т. п.).

10.3.11 На объекте в соответствии с технологическими, сантехническими, электротехническими и другими рабочими чертежами должна быть:

– выполнена прокладка магистральных трубопроводов и разводящих сетей с установкой арматуры для отбора теплоносителей к обогреваемым устройствам систем автоматизации, а также проложены трубопроводы для отвода теплоносителей;

– выполнена установка оборудования и проложены магистральные и разводящие сети для обеспечения средств автоматизации электроэнергией и энергоносителями (сжатым воздухом, газом, маслом, паром, водой и т. п.), а также проложены трубопроводы для отвода энергоносителей;

– проложена канализационная сеть для сбора стоков от дренажных трубных проводок систем автоматизации;

– выполнена заземляющая сеть, выполнены специальные контура заземления, в том числе и в гермообъеме;

– выполнена работа по монтажу систем пожаротушения.

10.3.12 Заземляющая сеть для технических средств / ПТС / ПТК должна отвечать требованиям проектной документации и требованиям предприятий-изготовителей оборудования технических средств / ПТС / ПТК.

10.3.13 Приемка помещений средств автоматизации для выполнения электромонтажных работ, оформляется актом сдачи помещений под электромонтажные работы.

10.4 Передача в монтаж средств автоматизации, изделий, материалов и технической документации

10.4.1 Порядок передачи в монтаж средств автоматизации, изделий, материалов и технической документации должен быть оговорен в Договоре между монтажной и эксплуатирующей организацией.

10.4.2 Принимаемые средства автоматизации, материалы и изделия должны соответствовать спецификациям, государственным стандартам, техническим условиям и иметь соответствующие сертификаты, технические паспорта/формуляры или другие документы, удостоверяющие их качество и иметь отметку для применения на АС.

Трубы, арматура и соединения для кислородных трубных проводок должны быть обезжирены, что должно быть указано в документации, подтверждающей проведение этой операции.

При приемке оборудования, материалов и изделий должна быть проверена комплектность, отсутствие повреждений и дефектов, сохранность окраски и специальных покрытий, сохранность пломб, наличие специального инструмента и приспособлений, поставляемых предприятиями-изготовителями совместно с оборудованием.

Устранение дефектов оборудования, обнаруженных в процессе приемки, должно осуществляется в соответствии с принятыми на АС процедурами.

10.4.3 Средства автоматизации, изделия и материалы должны передаваться в монтаж комплектно на технологическую систему, систему контроля и управления или для специальных помещений средств автоматизации – в соответствии с рабочей документацией.

10.4.4 Средства автоматизации, на которые истек нормативный срок хранения, указанный в паспорте или формуляре, принимаются в монтаж только после проведения предмонтажной ревизии, исправления дефектов и испытаний.

Результаты проведенных работ должны быть занесены в формуляры, паспорта и другую сопроводительную документацию.

Должен быть составлен акт о проведении указанных работ.

Передача средств автоматизации монтажным организациям, для выполнения электромонтажных работ, должна производится по акту приема-передачи. Ответственность за исправное состояние средств автоматизации в период производства электромонтажных работ несет монтажная организация.

Ответственность за сохранность оборудования, в помещениях принятых во временную эксплуатацию, несет эксплуатирующая организация.

10.5 Производство монтажных работ

10.5.1 Монтаж систем автоматизации должен производиться в соответствии с проектной документацией и с учетом требований к монтажу приведенных в поставляемой документации предприятий-изготовителей.

10.5.2 Работы по монтажу следует выполнять с использованием средств малой механизации, механизированного и электрифицированного инструмента и приспособлений. Номенклатура и тип инструмента и приспособлений применяемый для выполнения монтажа технических средств / ПТС / ПТК, должны соответствовать требованиям документации предприятий-изготовителей.

10.5.3 Работы по монтажу средств автоматизации должны осуществляться в две стадии (этапа).

10.5.3.1 На первой стадии следует выполнять:

– заготовку монтажных конструкций, узлов и блоков, элементов трубных, импульсных и электрических проводок, их укрупнительную сборку вне зоны монтажа;

– проверку наличия закладных конструкций, проемов, отверстий в строительных конструкциях и элементах зданий;

– проверку соответствия закладных конструкций и отборных устройств на технологическом оборудовании и трубопроводах требованиям проекта и документации предприятий-изготовителей средств автоматизации;

– проверку заземляющей сети и специального контура заземления требованиям проектной документации и документации предприятий-изготовителей средств автоматизации;

– закладку в сооружаемые фундаменты, стены, полы и перекрытия труб и глухих коробов для скрытых проводок; разметку трасс и установку опорных и несущих конструкций для электрических, трубных и импульсных проводок, исполнительных механизмов, стендов первичных измерительных преобразователей и т.д.;

10.5.3.2 На второй стадии необходимо выполнять:

– прокладку трубных, импульсных и электрических проводок по установленным конструкциям, установку стендов ПИП, технических средств / ПТС / ПТК;

– подключение трубных и импульсных проводок к стендам ПИП и электрических проводок к техническим средствам / ПТС / ПТК и проведение индивидуальных испытаний;

– монтаж первичных измерительных преобразователей, прошедших метрологическую поверку, на штатные места, как правило, должен выполняться перед началом индивидуального функционального опробования технологических систем, по указанию эксплуатирующей организации, кроме первичных измерительных преобразователей и показывающих приборов, поставляемых комплектно с оборудованием.

10.5.4 Смонтированные средства автоматизации, подлежащие заземлению согласно рабочей документации, должны быть присоединены к контуру заземления. При наличии требований предприятий-изготовителей оборудования, технических средств / ПТС / ПТК, они должны быть присоединены к контуру специального заземления в соответствии с проектной документацией.

10.5.5 Монтаж трубных проводок должен выполняться в соответствии с рабочей проектной документацией, кроме того, для импульсных трубных проводок при проектировании должна быть определена погрешность, которая должна быть подтверждена при сдаче из монтажа.

10.5.6 Монтаж кабельных конструкций, прокладка кабеля и подключение кабеля к герметичным проходкам, к техническим средствам / ПТС / ПТК должны выполняться в соответствии с рабочей проектной документацией, документацией и требованиями предприятий-изготовителей, под техническим надзором эксплуатирующей организации.

При прокладке кабеля в кабельных сооружениях и производственных помещениях все места прохода кабелей через стены и перекрытия, независимо от их конструктивного исполнения (модульные или трубные проходки, металлические короба и т.п.) должны временно уплотняться огнестойким материалом, разрешенным для временного уплотнения.

Все нарушенные в процессе прокладки кабеля временные уплотнения, должны ежедневно восстанавливаться по всей длине трассы после ежедневного окончания работ.

10.5.7 Монтаж технических средств / ПТС / ПТК, должен выполняться в соответствии с рабочей проектной документацией, документацией и требованиями предприятий-изготовителей, с выполнением требований СНиП 3.05.07, ПУЭ изд. 7, ОТТ 08042462, Правилами по охране труда при работе с инструментом и приспособлениями.

10.6 Индивидуальные испытания и приемка средств автоматизации из монтажа

10.6.1 К приемке рабочей комиссии предъявляются технические средства / ПТС / ПТК в объеме, предусмотренном рабочей документацией, и прошедшие индивидуальные испытания.

10.6.1.1 При индивидуальном испытании следует проверить:

– соответствие смонтированных технических средств / ПТС / ПТК рабочей документации, документации заводов изготовителей, федеральным нормам и правилам, действующим в атомной энергетике;

– трубные и импульсные проводки на прочность и плотность;

– сопротивления изоляции электропроводок.

10.6.1.2 При проверке смонтированного оборудования, технических средств / ПТС / ПТК на соответствие рабочей документации проверяется соответствие:

– мест установки первичных измерительных преобразователей и технических средств, их типов и технических характеристик, спецификации оборудования;

– способов установки первичных измерительных преобразователей и приборов требованиям проекта и эксплуатационным инструкциям;

– выполнения монтажа электрических, трубных и импульсных проводок рабочей документации;

– выполненной маркировки, технических средств / ПТС / ПТК требованиям проекта.

10.6.1.3 Испытание трубных проводок и импульсных проводок на прочность и плотность, а также проверку сопротивления изоляции электропроводок осуществляют в соответствии с СНиП 3.05.07.

10.6.1.4 После окончания работ по индивидуальному испытанию оформляется акт о приемки оборудования после индивидуального испытания, к которому прилагается производственная документация, указанная в СНиП 3.05.07.

10.6.1.5 Допускается передача монтажных работ под наладку отдельными системами или отдельными частями подсистем УС. Сдача оформляется актом о приемке оборудования после индивидуального испытания по СНиП 3.05.07.

10.6.2 Документация, предъявляемая рабочим подкомиссиям, на выполненные электромонтажные работы по средствам автоматизации определяется в соответствии с СНиП 3.05.07, СТО 1.1.1.03.003.0916.

10.6.3 После сдачи и индивидуальных испытаний рабочей подкомиссией составляется акт об окончании электромонтажных работ в соответствии с требованиями СНиП 3.05.07 и представляется на утверждение рабочей комиссии.

10.6.4 Средства автоматизации считаются переданными для проведения предпусковых наладочных работ после утверждения рабочей подкомиссией (комиссией) акта о приемке средств автоматизации для производства ПНР.

10.6.5 После приемки рабочей подкомиссией (комиссией) средств автоматизации, монтажная организация должна в согласованные с Заказчиком сроки передать Заказчику в одном экземпляре комплекты откорректированной технической документации.

10.6.6 Помещения, в которых закончены электромонтажные работы средств автоматизации, передаются по акту оперативному персоналу эксплуатирующей организации в постоянную эксплуатацию. Допуск и производство работ в

электроустановках расположенных в данных помещениях должны выполняться в соответствии с Правилами по охране труда при эксплуатации электроустановок.

11 Ввод управляющих систем в эксплуатацию

Ввод управляющих систем важных для безопасности АС осуществляется в соответствии с требованиями, изложенными в СТО 1.1.1.03.003.0914.

12 Эксплуатация управляющих систем энергоблока АС

12.1 Организация эксплуатации

12.1.1 Эксплуатация управляющих систем энергоблока АС представляет собой комплекс организационных и технических мероприятий, охватывающих все виды технической и административной деятельности направленных на поддержание управляющих систем в работоспособном состоянии во всех режимах работы энергоблока в соответствии с требованиями заводской и проектной документации, федеральными нормами и правилами действующими в атомной энергетике.

Для обеспечения работоспособности в период эксплуатации ТС / ПТС / ПТК управляющих систем энергоблока АС и средств автоматизации вспомогательных систем АС эксплуатирующая организация должна создать структурное подразделение – цех тепловой автоматики и измерений, либо другое подразделение с аналогичными функциями (далее – ЦТАИ).

В состав ЦТАИ должны входить участки, обеспечивающие организацию и проведение эксплуатации ТС / ПТС / ПТК управляющих систем энергоблока АС в соответствии с требованиями проектной и заводской документации, требованиями «Технологического регламента» и «Регламента технического обслуживания ТС / ПТС / ПТК УС энергоблока АС».

В проекте УС энергоблока АС должны быть даны основные положения по эксплуатации, в том числе определены требования к:

– структуре и составу ЦТАИ с учетом возможности организации планирования и проведения работ, устранению неисправностей, техническому обслуживанию и

ремонту, а также оперативному обслуживанию технических средств / ПТС / ПТК управляющей системы энергоблока АС;

– уровню квалификации ремонтного и оперативного персонала;

– задачам ЦТАИ;

– помещениям административного и технического персонала занятого обслуживанием ТС / ПТС / ПТК управляющей системы энергоблока АС;

– помещениям для проведения технического обслуживания и восстановления работоспособности оборудования в условиях АС;

– помещениям оперативного персонала;

– складским помещениям и помещениям хранения ЗИП;

– номенклатуре и количеству ЗИП для ТС / ПТС / ПТК, инструменту, средствам, обеспечивающим проведение технического и оперативного обслуживания, средствам, обеспечивающим восстановление работоспособности оборудования ТС / ПТС / ПТК в условиях АС, производственно-технической документации.

12.1.2 Требования к персоналу ЦТАИ обслуживающему ТС / ПТС / ПТК управляющей системы энергоблока АС

12.1.2.1 Основными задачами персонала являются обеспечение работоспособности и соответствия проектным характеристикам оборудования, технических средств / ПТС / ПТК управляющей системы энергоблока АС.

12.1.2.2 Технический персонал ЦТАИ должен обеспечить разработку мероприятий по обеспечению работоспособности УС энергоблока АС в течение всего срока эксплуатации, в том числе:

а) организационных мероприятий, включающих:

– подготовку и поддержания квалификации технического, ремонтного и оперативного персонала подразделения;

– комплектацию и приемку рабочих мест персонала в соответствии с проектными требованиями;

– разработку инструкций по эксплуатации, эксплуатационных схем, эксплуатационной и ремонтной документации на основании проектной документации и документации предприятий-изготовителей оборудования;

– разработку оперативных планов и карточек тушения пожара в помещениях с ТС / ПТС/ ПТК;

– разработку процедур по обеспечению сохранности оборудования, включая ЗИП, средства для проведения технического обслуживания и ремонта ТС / ПТС / ПТК;

– разработку эксплуатационной документации и процедур, обеспечивающих оперативное обслуживание ТС / ПТС / ПТК УС, при всех проектных режимах работы энергоблока АС;

– разработку документации обеспечивающей проведение технического обслуживания и планового ремонта технических средств / ПТС / ПТК управляющей системы энергоблока АС;

– разработку процедур по устранению неисправностей (дефектов) ТС / ПТС / ПТК УС в процессе эксплуатации энергоблока АС;

– разработку программ по поверке/калибровке, измерительных каналов УС в соответствии с требованиями проектной документации, документации предприятий-изготовителей;

– разработку документации обеспечивающей восстановление работоспособности ТС / ПТС / ПТК УС в условиях АС;

– разработку мероприятий по определению и продлению срока службы ТС и элементов ПТС / ПТК;

– разработку мероприятий по модернизации и реконструкции ТС / ПТС / ПТК УС энергоблока АС;

– разработку мероприятий обеспечивающих утилизацию, хранение и переработку элементов ТС / ПТС / ПТК не подлежащих восстановлению;

б) технических мероприятий, обеспечивающих проведение:

– всех видов планового технического обслуживания (ТО) ТС / ПТС / ПТК УС энергоблока АС в соответствии с программами ТО;

– всех видов ремонта ТС / ПТС / ПТК, в соответствии с эксплуатационной документацией;

– метрологической аттестации измерительных каналов УС энергоблока АС;

– сбора и анализ данных по надежности ТС / ПТС / ПТК УС энергоблока АС, ведению документации и информационной базы данных по состоянию и надежности оборудования УС энергоблока АС;

– анализа эффективности функционирования управляющей системы энергоблока АС и разработку предложений по совершенствованию;

– замены элементов ТС / ПТС / ПТК входящих в состав УС энергоблока АС;

– опробования и испытания СКУ, подсистем управляющей системы энергоблока АС при проведении пусковых операций, работе энергоблока на мощности и на энергоблоке, выведенном в ремонт;

– пополнения запасными элементами ТС / ПТС / ПТК.

Ремонтный и оперативный персонал должен быть подготовлен к выполнению работ на оборудовании ТС / ПТС / ПТК УС энергоблока АС в соответствии с требованиями СТО 1.1.1.01.0678.

Численность и квалификация ремонтного персонала должна обеспечивать выполнение:

– технического обслуживания ТС / ПТС / ПТК УС энергоблока АС, в соответствии с утвержденными графиками ТО, по согласованным и утвержденным в установленном на АС порядке программам;

– всех видов ремонта, ТС / ПТС / ПТК УС энергоблока АС в соответствии с требованиями проектной и заводской документации, по разработанным и утвержденным программам (картам ремонта оборудования).

Численность и квалификация оперативного персонала обслуживающего ТС / ПТС / ПТК УС энергоблока АС должна обеспечивать:

– подготовку рабочих мест для производства работ, допуск ремонтного эксплуатационного персонала и персонала подрядных организаций для производства работ, контроль за выполнением работ на оборудовании управляющей системы энергоблока АС, производство оперативных переключений в процессе выполнения работ, в соответствии с требованиями наряда / программы, приемку рабочих мест при прикрытии наряда и полном окончании работ;

– выполнение оперативных переключений на оборудовании управляющей системы энергоблока АС, по бланкам переключений / программам, в том числе:

а) вод/вывод из работы оборудования управляющей системы энергоблока АС;

б) проверку ТЗБиС (включая проверки при пусковых операциях и работе энергоблока на мощности);

в) подпитку уравнительных сосудов, продувку импульсных линий в соответствии с программами (для систем безопасности и систем, важных для безопасности программы должны быть согласованы с отделом ядерной безопасности АС);

– проведение ежесменных обходов оборудования УС энергоблока АС, в соответствии с действующими эксплуатационными инструкциями;

– устранение неисправностей на оборудовании УС энергоблока АС и проведение технического обслуживания в соответствии с требованиями технологического регламента безопасной эксплуатации энергоблока и инструкциями по эксплуатации технологического оборудования;

– готовность оборудования УС энергоблока АС к проведению регламентных проверок работоспособности систем безопасности и систем важных для безопасности, в соответствии с программами на работающем и выведенном в ремонт энергоблоке;

– выполнение технического обслуживания оборудования УС энергоблока АС, по программам технического обслуживания, в соответствии с утвержденными графиками.

12.1.3 Требования по готовности подразделения ЦТАИ к выполнению электромонтажных работ на энергоблоке

До начала электромонтажных работ на энергоблоке эксплуатирующая организация должна:

– на основании Типового положения о цехе тепловой автоматики и измерений АЭС обеспечить разработку согласование и утверждение Положений о структурных подразделениях по эксплуатации УС энергоблока АС, в которых должны быть указаны:

а) структура подразделения, с четким разграничением ответственности;

б) границы обслуживания оборудования УС энергоблока АС между подразделениями, а также зоны ответственности и порядок взаимодействия между ними при эксплуатации;

в) права, обязанности и ответственностью персонала, в том числе за ядерную, радиационную и пожарную безопасность, объем и порядок проверки знаний в соответствии с требованиями СТО 1.1.1.01.0678;

– разработать должностные инструкции персонала;

– организовать и открыть рабочие места для технического и ремонтного персонала;

– организовать и открыть рабочие места для оперативного персонала;

– провести обучение, стажировку и проверку знаний персонала;

– назначить лиц ответственных за выполнение технического надзора, при производстве электромонтажных и предпусковых наладочных работ (из числа технического персонала подразделений ЦТАИ), с правом участия в комиссиях по:

а) приемке помещений под монтаж и передачи оборудования для производства электромонтажных работ;

б) приемке электромонтажных работ и наладочных работ;

– обеспечить организацию приемку помещений закрепленных за ЦТАИ, для монтажа оборудования УС энергоблока АС, во временную эксплуатацию;

– ввести нарядно-допускную систему, в помещениях принятых во временную эксплуатацию, для выполнения электромонтажных работ.

12.1.4 Организация электромонтажных работ и приемка оборудования из монтажа персоналом ЦТАИ

12.1.4.1 Персонал ЦТАИ, обязан организовывать и контролировать производство работ по монтажу средств автоматизации в соответствии с графиком производства электромонтажных работ.

12.1.4.2 Распоряжением по ЦТАИ должны быть назначены ответственные лица из состава инженерно технических работников соответствующих подразделений, в соответствии с 12.1.3, за организацию и контроль производства электромонтажных

и наладочных работ. Права и обязанности персонала, по организации контролю выполнения монтажных и наладочных работ, должны быть определены в приказе по АС.

12.1.4.3 Персонал ЦТАИ ответственный за организацию и контроль выполнения электромонтажных работ, должен участвовать во входном контроле средств автоматизации в установленном на АС порядке. Для ПТС / ПТК систем безопасности и систем, важных для безопасности входной контроль должен проводиться совместно с представителем завода изготовителя.

12.1.4.4 Средства автоматизации прошедшие входной контроль должны быть переданы по акту монтажной организации.

12.1.4.5 Передача средств автоматизации, изделий, материалов и технической документации монтажным организациям, для выполнения электромонтажных работ, должна выполняться в соответствии с СНиП 3.05.07.

12.1.4.6 Ответственность за сохранность оборудования, в помещениях принятых во временную эксплуатацию, несет эксплуатирующая организация.

12.1.4.7 Допуск к выполнению электромонтажных и наладочных работ на оборудование, закрепленное за подразделением ЦТАИ - должен осуществлять оперативный персонал службы эксплуатации ЦТАИ.

12.1.4.8 Рабочие места оперативного персонала должны быть укомплектованы:

– списком электромонтажных и наладочных организаций имеющих право производства работ на оборудовании УС энергоблока АС, с указанием зон ответственности подрядных организаций. Выполнение работ монтажными и наладочными организациями на оборудовании СБ и СВБ должно быть подтверждено разрешением надзорного органа АС (копии разрешений должны находиться на рабочих местах оперативного персонала);

– списками персонала электромонтажных и наладочных организаций допущенных к выполнению работ на оборудовании УС энергоблока АС;

– схемами электропитания ТС / ПТС / ПТК УС энергоблока АС;

– проектной документацией на ТС / ПТС / ПТК УС энергоблока АС (объем устанавливает эксплуатирующая организация);

– документацией заводов изготовителей оборудования;

– нормативной и технической документацией обеспечивающей выполнение электромонтажных и пусконаладочных работ;

– средствами защиты персонала, инструментом, техническими средствами (перечень утверждается ГИС);

– ключами от помещений ТС / ПТС / ПТК принятых во временную эксплуатацию (распоряжение по ЦТАИ);

– оперативной документацией обеспечивающей выполнение этапа электромонтажных и пусконаладочных работ (перечень утверждается ГИС).

12.1.5 Требования по готовности ЦТАИ к выполнению предпусковых наладочных работ

12.1.5.1 До начала предпусковых наладочных работ на энергоблоке, ЦТАИ, должен быть укомплектован персоналом в соответствии со штатным расписанием. Персонал ЦТАИ должен пройти обучение, проверку знаний.

12.1.5.2 Для выполнения этапа предпусковых наладочных работ по средствам автоматизации, рабочие места оперативного персонала должны быть дополнительно укомплектованы:

– проектной документацией и документацией предприятий-изготовителей средств автоматизации в полном объеме;

– инструкциями по эксплуатации ТС / ПТС / ПТК и УС энергоблока АС в целом;

– регламентом эксплуатации ТС / ПТС / ПТК УС энергоблока АС;

– картами уставок ТЗБиС, картами настроек регуляторов;

– алгоритмами работы ТЗБиС;

– графиками проведения ПНР;

– программами и методиками: автономной и комплексной наладки ТС / ПТС / ПТК УС энергоблока АС; наладки измерительных каналов; аттестации измерительных каналов; наладки и индивидуальных испытаний арматуры и т.п. (ПМИ - должны быть согласованы и утверждены в установленном на АС порядке);

– журналом заявок на первичную подачу напряжения на оборудование ТС / ПТС / ПТК управляющей системы энергоблока АС;

– журналом готовности оборудования к этапам ПНР;

– журналом готовности арматуры к прокрутке с БПУ / РПУ, МЩУ;

– журналом учета проверки ТЗБиС;

– журналом учета состояний ТЗБиС;

– журналом учета прокрутки арматуры;

– журналом отписок готовности первичных измерительных преобразователей к вводу в работу;

– журналом заявок на производство ПНР;

– журналом неисправностей/дефектов оборудования ТС / ПТС / ПТК при ПНР;

– журналом учета и движения пусконаладочного ЗИП;

– журналом выдачи ключей от помещений принятых во временную и постоянную эксплуатацию;

– журналом заявок от смежных подразделений АС по готовности ТС / ПТС / ПТК УС энергоблока АС к этапам ПНР на тепломеханическом оборудовании;

– журналом технических решений при выполнении ПНР на ТС / ПТС / ПТК управляющей системы энергоблока АС;

– журналом технических и административных распоряжений ЦТАИ;

– журнал учета временных изменений проектных решений на технических средствах / ПТС / ПТК управляющей системы энергоблока АС.

12.1.5.3 Для выполнения этапа предпусковых наладочных работ на ТС / ПТС / ПТК УС энергоблока АС рабочие места ремонтного персонала должны быть дополнительно укомплектованы:

– графиками выполнения ПНР;

– программами и методиками автономной и комплексной наладки технических средств / ПТС / ПТК управляющей системы энергоблока АС, наладки измерительных каналов, наладки и индивидуальных испытаний арматуры и т.п.;

– проектной документацией и документацией предприятий – изготовителей и поставщиков программных и технических средств / ПТС / ПТК УС энергоблока АС (в полном объеме);

– инструкциями по эксплуатации ТС / ПТС / ПТК;

– регламентом эксплуатации технических средств / ПТС / ПТК управляющей системы энергоблока АС;

– картами уставок и алгоритмами работы ТЗБиС;

– картами настроек регуляторов;

– графиками проведения ПНР.

12.1.6 Требования к персоналу ЦТАИ при проведении предпусковых наладочных работ

12.1.6.1 Технический персонал ЦТАИ, обязан контролировать и обеспечивать проведение предпусковых наладочных работ на технических средствах / ПТС/ПТК управляющей системы энергоблока АС в том числе:

– контролировать график выполнения предпусковых наладочных работ (в зоне своей ответственности);

– принимать участие в совещаниях проводимых наладочными организациями и в оперативных совещаниях проводимых администрацией АС по вопросам ПНР;

– обеспечивать проверку каналов дистанционного управления арматурой и механизмами, проведение калибровки/поверки измерительных каналов;

– принимать участие в проведении испытаний средств автоматизации;

– участвовать в работе комиссий по приемке средств автоматизации на этапах автономной и комплексной наладки;

– участвовать в работе комиссий при приемке ТС / ПТС / ПТК УС энергоблока АС в опытно-промышленную эксплуатацию.

12.1.6.2 При проведении предпусковых наладочных работ оперативный персонал обязан:

– согласовывать порядок выполнения предпусковых наладочных работ по средствам автоматизации с технологическими подразделениями АС;

– выполнять все оперативные переключения на принятых в эксплуатацию средствах автоматизации;

– выполнять подготовку рабочих мест для наладочного и ремонтного персонала;

– производить допуск бригад к выполнению работ, надзор во время производства работ, приемку рабочих мест после окончания работ;

– контролировать монтаж и демонтаж временных схем (электропитания, управления, подпитки/продувки ПИП и т.п.)

– контролировать ведение журналов (см. 13.1.4);

– решать в оперативном порядке все вопросы, возникающие при выполнении пусконаладочных работ со смежными подразделениями АС;

– производить замену элементов технических средств / ПТС / ПТК вышедших из строя в процессе выполнения пусконаладочных работ;

– контролировать проведение работ по программам испытаний технических средств / ПТС / ПТК управляющей системы энергоблока АС.

12.1.7 Требования к ЦТАИ при опытно-промышленной эксплуатации оборудования технических средств / ПТС / ПТК УС энергоблока АС

12.1.7.1 К этапу опытно-промышленной эксплуатации рабочие места персонала ЦТАИ должны быть укомплектованы откорректированной по результатам ПНР технической документацией на ТС / ПТС / ПТК УС энергоблока АС, программами опытно-промышленной эксплуатации УС энергоблока АС.

12.1.7.2 Принятое в опытно-промышленную эксплуатацию оборудование СКУ управляющей системы энергоблока АС, должно эксплуатироваться в соответствии с инструкциями по эксплуатации, регламентом технического обслуживания технические средства / ПТС / ПТК управляющей системы энергоблока АС, технологическим регламентом безопасной эксплуатации энергоблока с соблюдением федеральных норм и правил, принятых в атомной энергетике.

12.1.7.3 Ввод в работу технические средства / ПТС / ПТК управляющей системы энергоблока АС должен выполняться по пошаговым программ согласованным с технологическими подразделениями АС и утвержденным в установленном на АС порядке.

12.1.7.4 Все переключения на оборудовании управляющей системы энергоблока АС должны выполняться оперативным персоналом, или ремонтным персоналом, если это оговорено в программах выполнения работ и/или в наряде на выполнение работ.

12.1.8 Требования к ЦТАИ при пусковых операциях на энергоблоке

12.1.8.1 К этапу ввода оборудования УС энергоблока АС в работу при пусковых операциях на энергоблоке, рабочие места персонала служб ЦТАИ должны быть укомплектованы:

– откорректированной по результатам ПНР и опытно-промышленной эксплуатации технической документацией на УС энергоблока АС;

– программами ввода в работу УС энергоблока АС в соответствии с программой пуска блока;

– графиком пуска энергоблока;

– пошаговыми программами проверок ТЗБиС при вводе в работу технологических систем и оборудования энергоблока (программы должны предусматривать проверки с воздействием на исполнительные механизмы);

– программами испытаний УС энергоблока АС совместно технологическим оборудованием энергоблока при пусковых операциях, физическом и энергетическом пуске;

– эксплуатирующей организацией должны быть сформированы дежурные бригады из числа ремонтного, монтажного, наладочного и шеф персонала для своевременного устранения неисправностей на оборудовании УС энергоблока АС (при необходимости дежурные бригады должны включаться в состав смены оперативного персонала ЦТАИ);

– приказ о привлечении ремонтного персонала и персонала подрядных организаций к проведению пусковых операций на энергоблоке должен быть утвержден ГИС и согласован с заинтересованными организациями;

– руководство дежурными бригадами, входящими в состав смены оперативного персонала ЦТАИ осуществляет начальник смены;

– все оперативные переключения на оборудовании УС энергоблока АС выполняет оперативный персонал ЦТАИ;

– допуск дежурных бригад, к выполнению работ на оборудовании УС энергоблока АС, оперативным персоналом ЦТАИ.

12.1.8.2 Требования, которым должны удовлетворять процедуры испытаний и опробований ТС / ПТС / ПТК управляющих систем энергоблока, должны быть

изложены в отдельном документе, который должен быть разработан в развитие настоящих «Общих положений».

12.1.8.3 Требования к содержанию и порядок разработки приемосдаточной и эксплуатационной документации на этапах ввода ТС / ПТС / ПТК УС энергоблока АС должны быть изложены в отдельных документах, которые должны быть разработаны в развитие настоящих «Общих положений».

13 Внесение изменений в УСВБ

13.1 Общие положения

13.1.1 На АС должен быть регламентирован порядок внесения изменений в проект УСВБ и процедуры внесения изменений во все подчиненные проектные решения, оборудование, программное обеспечение и документацию.

13.1.2 Процедура внесения изменений затрагивает следующие части проекта УСВБ:

– проектную и рабочую документацию;

– проектные базы данных;

– видеокадры;

– компоненты и элементы конфигурации аппаратных средств;

– компоненты и элементы технических и программных средств оборудования УСВБ;

– системные и прикладные программные средства, программную документацию;

– схемные и аппаратные решения;

– логику формирования ТЗБ, регуляторов и пошаговых программ.

13.1.3 Под изменением проектной и рабочей документации, проектных баз данных, видеокадров, компонентов и элементов конфигурации, системных и прикладных программных средств и программной документации следует понимать любое изменение (дополнение, исправление, удаление и т.п.) каких-либо средств и/или данных.

13.1.4 Изменения, не приводящие к изменению проектных решений, являются настройкой системы. Процедура внесения подобных изменений должна быть

формализована на АС отдельной совокупностью правил и предписаний с учетом раздела 13.4 настоящих общих технических требований.

13.1.5 При любых изменениях, вносимых в УСВБ, должно обеспечиваться взаимное соответствие между документацией и оборудованием.

13.2 Основание и цели внесения изменений

13.2.1 Целями внесения изменений в проект УСВБ являются:

– устранение ошибок и несоответствий в проектной и рабочей документации;

– устранение ошибок в работе ПТК, выявленных в процессе эксплуатации;

– проведение модернизации УСВБ с целью повышения безопасности, устойчивости работы и ремонтопригодности оборудования.

13.2.2 Основанием для внесения изменений в проект УСВБ являются решения (технические решения), оформленные в соответствии с РД ЭО 1.1.2.01.0740 и локальными нормативными и организационно-распорядительными документами АС.

13.2.3 В решении (техническом решении) должны быть указаны ответственные за все этапы внесения изменений, а также информация по финансированию работ, связанных с внедрением изменения.

13.2.4 Все документы, вновь разрабатываемые или подвергаемые изменению в процессе внесения изменений в проект УСВБ, должны пройти процедуру согласования и утверждения в установленном порядке.

13.2.5 Ответственные за согласование вносимых изменений с поставщиками основного оборудования и необходимость внесения изменений в УДЛ определяются на АС в установленном порядке.

13.3 Классификация изменений

Исходя из состава и структуры, а также системы конструирования и проектирования УСВБ, изменения можно разделить на виды, отраженные на рисунке 1.



Рисунок 1 – Виды изменений проекта УСВБ

13.3.1 Изменение документации проекта

13.3.1.1 Документация, которая может быть изменена в связи с принятием решения об изменении:

– проектная документация;

– рабочая документация;

– эксплуатационная документация;

– программная документация;

– технические задания (частные технические задания) на систему(ы) (средства);

– обоснование безопасности АС и РУ;

– регламент эксплуатации УСВБ;

– технологические инструкции;

– руководства пользователя;

– программы и методики испытаний.

13.3.1.2 Внесение изменений в документы должно проходить в соответствии с принципами, приведенными в ГОСТ 2.503, ГОСТ 19.603.

13.3.1.3 Все участники создания системы или ее части должны быть извещены о внесении изменения в документацию проекта.

13.3.2 Внесение изменений в аппаратную часть

13.3.2.1 Внесение изменений в аппаратную часть заключаются в изменении конфигурации технических средств (замена, добавление, исключение модулей/контроллеров) с заменой, при необходимости, лицензионных соглашений на использование (сертификатов).

13.3.2.2 Если заменяемое ТС имеет в своем составе прикладное программное обеспечение, должна быть проведена процедура его установки на заменяемое техническое средство.

13.3.2.3 Изменение внутришкафного монтажа без изменения принципиальной схемы, не требует оформления решения (технического решения).

13.3.2.4 Изменения в схемотехнические решения, изменения схем подключения производятся по решению (техническому решению).

13.3.3 Изменение технологических алгоритмов ПТК

13.3.3.1 Причинами изменений технологических алгоритмов ПТК могут являться:

– устранение проектных ошибок;

– поставка оборудования с измененными характеристиками;

– развитие и усовершенствование алгоритмов.

13.3.3.2 Изменение технологических алгоритмов производятся по решению (техническому решению) и согласовываются с генеральным проектировщиком АС, главным конструктором РУ и научным руководителем в пределах их зон ответственности.

Примечание - Внесение изменений в настроечные параметры алгоритмов управления оборудованием не является изменением технологических алгоритмов.

13.3.4 Изменения проектной базы данных

13.3.4.1 Проектная база данных является проектным документом проектировщика системы и представляет собой набор таблиц, характеризующих устройства, с которыми ПТК связаны входными и выходными сигналами.

13.3.4.2 В качестве источников входных и выходных сигналов выступают:

– датчики аналоговых и дискретных сигналов, а также другие устройства, в частности цифровые, формирующие входные сигналы ПТК;

– электроприводы исполнительных механизмов (клапаны, задвижки, двигатели);

– внешние потребители информации ПТК, напрямую не связанные с формированием управляющих воздействий на энергоблок (традиционные показывающие приборы, регистраторы, табло сигнализации);

– сигналы технологических алгоритмов ПТК.

13.3.4.3 Изменения проектной базы данных УСВБ могут потребовать:

– непосредственное изменение исходных данных (добавление, удаление, изменение точек контроля, изменение уставок сигнализации, диапазонов датчиков и др.);

– изменение структуры базы данных (исключение/добавление отдельных полей, таблиц, связей, хранимых процедур).

13.3.4.4 Основаниями для инициации процесса внесения изменений в проектную базу данных УСВБ могут являться:

– изменение состава технических средств;

– изменение количества или марки точек контроля, отображения;

– изменение количества технологических алгоритмов и состава их входных/выходных сигналов.

13.3.5 Изменение программных средств

13.3.5.1 Под изменением программных средств подразумевается:

– обновление (модификация) программных средств, системного программного обеспечения, прикладного программного обеспечения, программных приложений, в том числе видеокадров;

– устранение программных ошибок и/или изменение функциональных возможностей программы (в части изменения состава, структуры, режима работы и класса решаемых задач техническими средствами);

– изменение видеокадров в части добавления элементов контроля, управления, пиктограмм, изменение структурных схем, надписей, осуществление переприв язки объектов.

13.3.5.2 Изменение настроечных величин в программных средствах технических средств не является изменением программных средств УСВБ.

13.3.5.3 Процедура изменения программных средств должна сопровождаться выпуском новой (n+1) версии программного обеспечения.

13.3.5.4 В ходе проведения процедуры внесения изменений в программное обеспечение должны быть предприняты организационные и технические меры по обеспечению безопасности.

13.3.5.5 До и после процесса внесения изменений должно быть предусмотрено создание резервных копий (образов) систем (отдельных программ), над которыми проводятся описываемые операции.

13.3.5.6 Выпуск разработчиком каждой новой версии программного обеспечения, содержащего изменения по отношению к предыдущей, актуальной версии, должен инициировать передачу заказчику оптических носителей с данным ПО в установленном на АС порядке.

13.4 Порядок внесения изменений, не требующих корректировки проектной документации

13.4.1 К изменениям, не требующим корректировки проектной документации, как правило, относятся:

– изменения настроек технических средств и программного обеспечения УСВБ, системные изменения (например, изменения параметров систем диагностики данных и самодиагностики оборудования ТПТС);

– изменения настроечных параметров автоматических регуляторов, настроечных параметров исполнительных механизмов и элекроприводной арматуры (время хода, время переключения);

– изменения настроечных параметров каналов обработки сигналов с датчиков механизмов транспортно-технологического оборудования;

– корректировка ошибок GET-проекта в части параметризации функциональных блоков, а также параметризации и генерации кода функциональных и центральных модулей ТПТС;

– изменения видеокадров, не затрагивающие изменения технологических схем и алгоритмов (изменения в части настройки элементов управления и отображения и т.п.).

13.4.2 Инициация процесса внесения изменений, подпадающих под данную категорию, должна производиться в установленном на АС порядке с подготовкой исходных данных, согласованием со всеми заинтересованными структурными подразделениями и утверждением их главным инженером АС.

13.4.3 Изменения, не требующие корректировки проектной документации, допускается вносить без оформления решения (технического решения).

13.4.4 Работы по внесению изменений оформляются и проводятся в соответствии с действующей нарядно-допускной системой АС.

13.4.5 В случае необходимости должны быть разработаны дополнительные рабочие программы, определяющие порядок проведения работ на оборудовании блока.

13.4.6 Результаты работ по внесению изменений оформляются в виде выписки в журнал учета изменений (журнал состояния системы) ЦТАИ.

13.4.7 Корректировка эксплуатационной документации должна быть произведена до внесения изменений.

13.5 Порядок внесения изменений, требующих корректировки проектной, рабочей или конструкторской документации

13.5.1 Этапы работ

Работа по внесению изменений должна выполняться по следующим этапам:

– оповещение всех заинтересованных сторон о необходимости внесения изменений в систему (или наличие оформленного требования от производителя основного оборудования, главного конструктора, проектанта);

– проведение совещания между заинтересованными сторонами, принятие решения (при необходимости);

– подготовка исходных данных в виде задания на изменение, утвержденного ГИС;

– оформление решения (технического решения);

– подготовка и оформление рабочей документации, включая техническое задание заводам-изготовителям на корректировку ПТК (при необходимости);

– оформление, при необходимости, дополнений к проектным материалам ООБ, технического проекта УСВБ;

– внесение изменений;

– проведение требуемого монтажа, ПНР и корректировка/выпуск ЭД;

– ввод в эксплуатацию, включая проведение необходимых испытаний.

Примечание: В зависимости от назначения, специфических особенностей проводимых изменений (изменения не затрагивают проектные решения, конструкторскую документацию или программное обеспечение) допускается вводить дополнительные, исключать или объединять рассмотренные выше этапы.

13.5.2 Подготовка исходных данных

13.5.2.1 Исходные данные готовятся для формирования решения (технического решения) и представляют собой задание (технологическое задание) на внесение изменений в проект УСВБ оформленное по установленной на АС форме.

13.5.2.2 Исходные данные должны содержать сведения о влиянии предлагаемых изменений на безопасность и условия действия лицензии на сооружение и эксплуатацию энергоблока АС.

13.5.2.3 Исходные данные должны содержать информацию необходимую для диагностики и идентификации исходных событий, приведших к необходимости внесения изменений (признаки ошибок, неоднозначности, неполноты или противоречивости информации исходных событий, коренные причины несоответствий).

13.5.2.4 Исходные данные для внесения изменений утверждаются главным инженером АС и передаются в ЦТАИ для оформления решения (технического решения).

13.5.3 Оформление решения (технического решения)

Порядок разработки, оформления и учета решений (технических решений) определены РД ЭО 1.1.2.01.0740 и локальными нормативными, организационно-распорядительными документами АС.

13.5.4 Оформление изменений

13.5.4.1 На основании решений (технических решений) Генпроектировщиком, при необходимости, вносятся изменения в рабочую документацию, в том числе оформляются задания заводам-изготовителям.

13.5.4.2 После утверждения решение (техническое решение) направляется всем заинтересованным сторонам для внесения изменений в документацию (рабочую, эксплуатационную, заводскую).

13.5.5 Подготовка и внесение изменений

Процедуры внесения изменений в оборудование УСВБ должны быть формализованы в локальных нормативных документах АС с учетом следующих положений:

13.5.5.1 Необходимый объём и качество выполняемых работ по решению (техническому решению) подтверждается актами верификации и валидации, предоставляемыми организацией, подготовившей изменения.

13.5.5.2 Выполнение работ производится по программе работ, определяющей методы, средства и порядок выполнения работ, установленных в решении (техническом решении). Работы по программе выполняются по разрешенной главным инженером АС заявке и в соответствии с нарядно-допусконой системой АС.

13.5.5.3 Внесение изменений в ТС и ПО УСВБ производится персоналом ЦТАИ или персоналом завода-изготовителя совместно с персоналом (под контролем персонала) ЦТАИ;

13.5.5.4 Проверка внесённых изменений выполняется персоналом ЦТАИ совместно с персоналом завода-изготовителя по утвержденной программе.

13.5.5.5 После подтверждения правильности внесённых изменений, при необходимости, производится аппаратная доработка оборудования и обновление программного обеспечения узлов из комплекта ЗИП.

13.5.5.6 Резервное копирование ПО, учет и хранение резервных копий и отчетной документации по внесению изменений (акты о выполнении изменений,

журналы внесения изменений, сопроводительные письма и т.п.) ведется назначенными в ЦТАИ ответственными лицами в установленном на АС порядке.

13.5.6 Оформление акта

13.5.6.1 Завершающим этапом внедрения изменения является подготовка акта выполненных работ по установленной на АС форме.

13.5.6.2 В акте должны быть указаны номера рабочей документации, номера формуляров ТС, регистрационные номера записей (протоколов) выполнения необходимых испытаний, т.е. всех документов, изменение которых было предусмотрено решением (техническим решением).

14 Модернизация

Модернизация управляющих систем важных для безопасности АС осуществляется в соответствии с требованиями, изложенными в СТО 1.1.1.04.003.0542.

15 Обеспечение информационной безопасности

В эксплуатирующей организации дополнительно должны быть разработаны документы, определяющие требования ИБ СКУ АС при проектировании, конструировании, изготовлении, монтаже, наладке и эксплуатации, а также определяющие базовый набор мер ИБ.

15.1 Общие требования к информационной безопасности СКУ АС

15.1.1 На всех предприятиях, участвующих в проектировании, конструировании, изготовлении, монтаже, вводе в эксплуатацию и эксплуатации СКУ энергоблока АС, должны быть назначены ответственные (выделенное структурное подразделение или лицо) за ИБ СКУ. Специалисты должны обладать достаточным объемом знаний в части ИБ и функционирования СКУ, позволяющим выполнять свои должностные обязанности. Специалисты должны непосредственно отвечать за соблюдение требований и политик ИБ СКУ на этапах проектирования,

конструирования, изготовления, монтажа, ввода в эксплуатацию и эксплуатации АСУ ТП.

15.1.2 В ПОК АС должны быть внесены изменения, необходимые для обеспечения требуемого уровня качества СКУ АС с учетом требований ИБ. Проверки соблюдения требований ИБ СКУ должны быть составной частью аудита по обеспечению качества.

15.1.3 В договорных обязательствах организаций, участвующих в жизненном цикле СКУ, должны быть включены положения о неразглашении информации, связанной с ИБ СКУ.

15.2 Основные требования на этапе проектирования

15.2.1 Проектная организация должна определить перечень и классифицировать защищаемые элементы СКУ.

15.2.2 При необходимости проектная организация может предъявить дополнительные требования к СКУ в части ИБ./*

15.2.3 Разрабатываемая на этапе проектирования документация по СКУ должна содержать раздел по ИБ.

15.2.4 Проектная организация должна определить перечень сигналов и данных, передаваемых из СКУ в сторонние системы.

15.3 Основные требования на этапе конструирования

15.3.1 Главный конструктор СКУ должен разработать частную модель угроз и провести оценку рисков ИБ. По итогам оценки рисков может быть выполнена корректировка структурно-функциональных характеристик СКУ и проведена адаптация базового набора мер ИБ. При необходимости конструктор СКУ может предъявить дополнительные требования к ИБ. Результаты оценки рисков должны быть документированы, включены в состав конструкторской документации СКУ и согласованы с эксплуатирующей организацией.

15.3.2 На этапе конструирования главный конструктор СКУ должен определить архитектуру СКУ.

15.3.3 При определении архитектуры СКУ должны учитываться структурно-функциональные характеристики СКУ, состав СКУ, физические, логические, функциональные и технологические взаимосвязи в СКУ, взаимодействие со сторонними системами, а также другие особенности её построения и функционирования с учетом требований ИБ.

15.3.4 В сторонние системы должен передаваться только определенный на этапе проектирования перечень сигналов.

15.3.5 Вся документация, разрабатываемая на этапе конструирования, должна соответствовать требованиям, предъявляемым на этапе проектирования, и содержать раздел ИБ (включая ЧТЗ на подсистемы СКУ).

15.3.6 Главный конструктор должен предъявить требования заводам-изготовителям на реализацию адаптированного набора мер ИБ.

15.4 Основные требования на этапе изготовления

15.4.1 При изготовлении элементов СКУ и СЗИ завод-изготовитель должен выполнить требования ИБ, предъявляемые проектантом и конструктором СКУ.

15.4.2 Завод-изготовитель должен разработать частную модель угроз элементов СКУ и провести оценку рисков реализации угроз. По итогам оценки рисков может быть проведено уточнение адаптированного базового набора мер ИБ и, при необходимости, набор мер ИБ может быть дополнен.

15.4.3 Результаты оценки рисков должны быть документированы, включены в состав документации на элементы СКУ и согласованы с эксплуатирующей организацией.

15.4.4 При разработке ПО, изготовлении ТС, выборе ТС и ПО серийного производства должны учитываться требования ИБ.

15.4.5 Завод-изготовитель элементов СКУ должен разработать следующую документацию по ИБ:

– инструкции по эксплуатации, включающие инструкции по внесению изменений и обновлению ПО, инструкции по администрированию системы,

инструкции по обслуживанию и ремонту системы, инструкции, описывающие замену/ремонт сетевых устройств;

– инструкции по настройке штатных механизмов защиты ОС и ПО, антивирусной защиты, межсетевых экранов, инструкции по эксплуатации систем сетевого мониторинга и контроля целостности;

– обоснование применения зарубежных ПО, ТС (их комплектующих) и ОС (при необходимости);

– отчет о верификации и валидации ПО совместно с методикой верификации и валидации;

– отчет о проверке надежности и безопасности ПО и ТС совместно с программами испытаний;

– программы испытаний элементов СКУ, включающие проверки на соответствие требованиям ИБ.

15.5 Приемо-сдаточные испытания СКУ в части ИБ

15.5.1 Приемо-сдаточные испытания СКУ в части ИБ проводятся по программе испытаний согласованной с заинтересованными организациями и утвержденной заказчиком.

15.5.2 В ходе приемо-сдаточных испытаний должен быть проведен комплекс организационных и технических мероприятий (в том числе испытаний), в результате которых подтверждается соответствие СКУ техническому заданию в части ИБ.

15.5.3 Подтверждение соответствия элементов СКУ в части ИБ должно выполняться в соответствии с РД ЭО 1.1.2.01.0713.

15.5.4 В качестве исходных данных при приемо-сдаточных испытаниях используются: частные модели угроз ИБ, ЧТЗ на элементы СКУ, проектная и эксплуатационная документация, программы испытаний.

15.5.5 По результатам приемо-сдаточных испытаний СКУ в части ИБ составляется протокол, на основании которого делается вывод о соответствии СКУ требованиям ТЗ в части ИБ и о готовности СКУ в части ИБ к отправке на АС.

Библиография

[1] IEC/IEEE 60780-323 «Nuclear facilities - Electrical equipment important to safety - Qualification»

[2] NS-G-1.3 «Instrumentation and Control Systems Important to Safety in Nuclear Power Plants. Safety guide»

[3] IEEE Std 1012 «Standard for System and Software Verification and Validation»

[4] ANSI/ANS-10.4-2008 «Verification and Validation of Non-Safety-Related Scientific and Engineering Computer Programs for the Nuclear Industry»

[5] 58413824.23512.001-390.РД-01-2002.М «Верификация и валидация программных средств управляющих систем, важных для безопасности атомных станций. Общие требования. Руководящий документ»

[6] NS-G-1.1 «Software for Computer Based Systems Important to Safety in Nuclear Power Plants. Safety guide»

[7] IEC 60987-2013 Nuclear power plants – Instrumentation and control important to safety – Hardware design requirements for computer-based systems - Edition 2.1 Consolidated Reprint

Лист согласования

ОТТ 1.1.3.10.1446-2018 «Атомные станции. Управляющие системы, важные для безопасности. Создание, модернизация и эксплуатация. Общие технические требования»

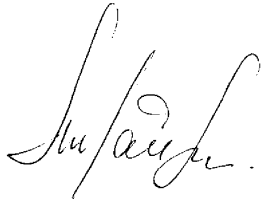
И. о. заместителя директора по производству и эксплуатации АЭС – директора Департамента по эксплуатационной готовности новых АЭС



А.А. Буданов

13.06.2018

gost.e-ecolog.ru



М.А. Михайлова

